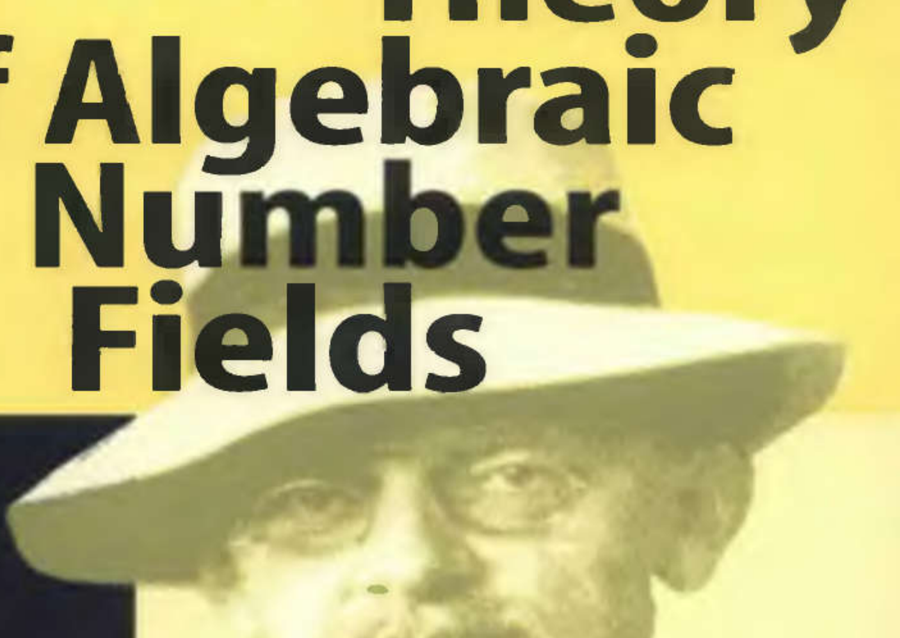
DAVID HILBERT

The Theory of Algebraic Number Fields

Zahlbericht



Springer



HILBERT

The Theory of Algebraic Number Fields

This book is a translation into English of Hilbert's *Theorie der algebraischen Zahlkörper*, best known as the *Zahlbericht*, first published in 1897, in which he provided an elegantly integrated overview of the development of algebraic number theory up to the end of the nineteenth century. The Zahlbericht provided also a firm foundation for further research in the subject. It is based on the work of the great number theorists of the nineteenth century. The Zahlbericht can be seen as the starting point of all twentieth century investigations in algebraic number theory, reciprocity laws and class field theory. For this English edition by I. T. Adamson an Introduction has been added by F. Lemmermeyer and N. Schappacher.

ISBN 3-540-62779-0

9 783540 627791

http://www.springer.de

Springer
Berlin
Heidelberg
New York
Barcelona
Budapest
Hong Kong
London
Milan
Paris
Singapore
Tokyo

David Hilbert

The Theory of Algebraic Number Fields

Translated from the German by Iain T. Adamson
With an Introduction
by Franz Lemmermeyer and Norbert Schappacher

Springer

Iain T. Adamson

Department of Mathematics
The University of Dundee
Dundee DD1 4HN, Scotland
email: iadamson@mcs.dundee.ac.uk

Franz Lemmermeyer

Universität des Saarlandes
Fachbereich Mathematik
Pf 15 11 50
D-66041 Saarbrücken, Germany
email: franz@math.uni-sb.de

Norbert Schappacher

Université Louis Pasteur
UFR de Mathematiques
et Informatique
7 rue R. Descartes
F-67084 Strasbourg, France
email: schappa@math.u-strasbg.fr

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Hilbert, David:
The theory of algebraic number fields / David Hilbert. Transl. from the German by Iain T. Adamson. With an introd. by Franz Lemmermeyer and Norbert Schappacher. - Berlin; Heidelberg; New York; Barcelona; Budapest; Hong Kong; London; Milan; Paris; Singapore; Tokyo: Springer, 1998
Einheitssacht.: Die Theorie der algebraischen Zahlkörper <engl.>
ISBN 3-540-62779-0

Mathematics Subject Classification (1991): 11-02, 11-03, 11Rxx

ISBN 3-540-62779-0 Springer-Verlag Berlin Heidelberg New York

Printed in Germany

Typeset in LaTeX by the translator
Cover design: Erich Kirchner, Heidelberg

SPIN 10570837 41/3143 - 5 4 3 2 1 0 - Printed on acid-free paper

Translator's Preface

Constance Reid, in Chapter VII of her book *Hilbert*, tells the story of the writing of the *Zahlbericht*, as his report entitled *Die Theorie der algebraischen Zahlkörper* has always been known. At its annual meeting in 1893 the Deutsche Mathematiker-Vereinigung (the German Mathematical Society) invited Hilbert and Minkowski to prepare a report on the current state of affairs in the theory of numbers, to be completed in two years. The two mathematicians agreed that Minkowski should write about rational number theory and Hilbert about algebraic number theory. Although Hilbert had almost completed his share of the report by the beginning of 1896 Minkowski had made much less progress and it was agreed that he should withdraw from his part of the project. Shortly afterwards Hilbert finished writing his report on algebraic number fields and the manuscript, carefully copied by his wife, was sent to the printers. The proofs were read by Minkowski, aided in part by Hurwitz, slowly and carefully, with close attention to the mathematical exposition as well as to the type-setting; at Minkowski's insistence Hilbert included a note of thanks to his wife.

As Constance Reid writes, "The report on algebraic number fields exceeded in every way the expectation of the members of the Mathematical Society. They had asked for a summary of the current state of affairs in the theory. They received a masterpiece, which simply and clearly fitted all the difficult developments of recent times into an elegantly integrated theory. A contemporary reviewer found the *Zahlbericht* an inspired work of art; a later writer called it a veritable jewel of mathematical literature".

Nearly 70 years after the publication of the *Zahlbericht* we find Serge Lang writing that "expositions of the theory of number fields are principally conditioned by it and by Artin's *Algebraic numbers and algebraic functions*" and that the plan of his own book *Algebraic numbers* is in a certain sense still more or less that used by Hilbert. "The Bericht", he writes, "contains a large number of computations and examples which still make it very pleasurable to read." And in his 1970 book *Algebraic number theory* Lang encourages his readers to study *inter alia* older books like Hilbert's *Zahlbericht*, commenting that "It seems that over the years, everything that has been done has proved useful, theoretically or as examples, for the further development of the theory.

Old, and seemingly isolated special cases have continuously acquired renewed significance, often after half a century or more."

It is surprising that no English translation of the *Zahlbericht* has ever been published. Whether we like it or not it seems that English has become the almost universal language of mathematics; so it is not inappropriate to mark the centenary of this magisterial work by translating it into English. I have not tried to reproduce Hilbert's German style in English; in particular I have not imitated Hilbert's characteristic Prussian use of the singular where it seems more natural in English to use the plural. I have followed Hilbert in numbering the sections, theorems and lemmas consecutively throughout the whole book – if only because no one can be expected after 100 years to refer to Hilbert's Theorem 90 as Theorem 15.1. My aim has been to produce an English version approaching the clarity I was taught to strive after at the feet of my master, Emil Artin, when I prepared the notes of his *Algebraic numbers and algebraic functions* (the *Zahlbericht* of his day) in 1950–51. It pleases me to think that having begun my career by writing down the New Testament, so to speak, I should end it by translating the Old.

I have to thank Springer-Verlag and especially their Mathematics Editor, Dr Catriona Byrne, for agreeing to publish this translation of the *Zahlbericht* and for engaging Franz Lemmermeyer and Norbert Schappacher to write the very scholarly introduction; they also made a number of helpful comments on the translation and modernised Hilbert's References. In preparing the translation I have had help and advice from four English-speaking Germanists, Margaret Adamson, Alison Andrews, Katherine Baxter and Alex Robertson and three German native speakers, Damaris Hermey, Sven Leyffer and Christine Zoppke Donaldson: for all their assistance I am very grateful – I need hardly say that any inaccuracies or infelicities in the translation are entirely my responsibility. My friend Murray Macbeath has very kindly read and commented helpfully on much of my translation and I want to record my thanks for this. Not for the first time I have to express my gratitude to Nick Dawes for his assistance with the intricacies of LaTeX. Karl-Friedrich Koch has been very helpful in turning the LaTeX files into the finished book.

My wife has been a constant source of encouragement while I have been working on this project; for her support in this, as in everything I do, I am deeply grateful – and at least I did not expect her to follow Frau Hilbert's example and copy out the manuscript!

Dundee, Scotland, 10 April 1997 IAIN T. ADAMSON

Hilbert's Preface

Number theory is one of the oldest branches of mathematics and the human mind became aware very early of some quite deep properties of the natural numbers. Nevertheless its status as an independent and systematic science is entirely an achievement of modern times.

From time immemorial number theory has been renowned for the simplicity of its foundations, the precision of its concepts and the clarity of its truths; it has enjoyed these properties from the very beginning, whereas other branches of mathematics had to pass through a more or less extended development before the desire for confidence in the ideas and rigour in the proofs was met completely.

So we are not surprised by the great enthusiasm which this subject has inspired among its devotees of all times. "Nearly all mathematicians who take up their time with number theory," says Legendre in describing Euler's love for the subject, "give themselves up to it with a certain passion." We remember too the reverence which our master Gauss felt for the science of arithmetic, as, when he first succeeded in his desire to prove an outstanding arithmetic result, "the fascination of this investigation so enthralled him that he could not escape from it," and when he praised Fermat, Euler, Lagrange and Legendre as "men of incomparable glory" since they "have unlocked the door of the sanctuary of this divine science and have shown with what abounding riches it is filled."

A special feature of number theory is that we often encounter difficult proofs for simple results easily understood intuitively. "This," says Gauss, "is precisely what gives the higher arithmetic its fascinating charm, what made it the favourite science of the early surveyors, not to speak of its inexhaustible store of riches, in which it so far excels all other branches of mathematics."

Lejeune Dirichlet's love for arithmetic is also well-known. We know too how Kummer devoted his scholarly activity before all else to number theory; and Kronecker gave expression to the essence of his mathematical perception in the words "God made the natural numbers; everything else is humans' work."

With its simple prerequisites number theory is surely the field of mathematical knowledge whose results are easiest to understand. But to grasp and master completely the concepts and methods of proof in arithmetic

requires a high degree of facility in abstract thinking, and this fact is sometimes advanced as a reproach against the subject. In my opinion, however, all other branches of mathematics demand at least as great capacity for dealing with abstraction – assuming, that is, that we lay the foundations for them with the rigour and completeness which is really necessary.

As for the position of number theory within the whole of mathematics, Gauss, in the preface to his *Disquisitiones arithmeticæ*, still understands it as a theory of natural numbers, with all imaginary numbers strictly excluded. Accordingly he did not classify cyclotomy as number theory properly speaking; but he added that "its principles are derived purely and simply from the higher arithmetic." Along with Gauss, both Jacobi and Lejeune Dirichlet repeatedly and emphatically express their surprise at the close connexion between number-theoretic questions and algebraic problems, in particular the problem of cyclotomy. The central reason for this connexion is nowadays completely clear. Namely, the theory of algebraic numbers and the Galois theory of equations both have their roots in the theory of algebraic fields, and the theory of number fields has come to be the most essential part of modern number theory.

The credit for having sown the first seeds of the theory of number fields also belongs to Gauss. Gauss recognised that the real source of the laws of biquadratic residues lay in an "extension of the field of arithmetic" as he put it, namely the introduction of integral imaginary numbers of the form $a + bi$; he posed and solved the problem of carrying over to these complex integers all the theorems of ordinary number theory, especially properties concerning divisibility and congruence relations. By a systematic development of this notion in the light of new far-reaching ideas of Kummer, Dedekind and Kronecker later arrived at the present-day theory of algebraic number fields.

It is not only with algebra, however, but also with function theory that number theory enjoys intimate reciprocal relationships. We recall the numerous remarkable analogies which subsist between certain results in the theory of number fields and the theory of algebraic function fields of one variable; we think too of the profound investigations of Riemann by which the answer to the question of the distribution of prime numbers is made to depend upon knowledge of the zeros of a certain analytic function. Again, the transcendence of the numbers e and π is an arithmetic property of a certain analytic function, namely the exponential function. Finally, the important and far-reaching method devised by Lejeune Dirichlet for the determination of the class number of a number field rests on analytic foundations.

At the deepest level too, periodic functions and certain functions with linear self-transformations touch upon the very essence of number; thus the exponential function $e^{2\pi iz}$ is to be understood as the *invariant* for the rational integers in the sense that it is the fundamental solution of the functional equation $f(z+1) = f(z)$. Furthermore Jacobi had already noticed the close connexion between the theory of elliptic functions and the theory of quadratic

irrationalities; he had even suggested that in Gauss's work the idea mentioned above of introducing imaginary integers of the form $a+bi$ does not spring from purely arithmetic grounds but was called for by Gauss's contemporaneous study of the lemniscate functions and their complex multiplication. Elliptic functions for suitable values of their periods and elliptic modular functions in all cases are the invariants of the integers of some fixed imaginary quadratic number field. These functions which we have called invariants have the power to produce solutions to certain profound and difficult problems concerning the corresponding number fields; and, conversely, the theory of elliptic functions is indebted to these arithmetic ideas and applications for a new stimulus.

Thus we see how far arithmetic, the Queen of mathematics, has conquered broad areas of algebra and function theory and has become their leader. The reason that this did not happen sooner and has not yet developed more extensively seems to me to lie in this, that number theory has only in recent years become known in its maturity. Even Gauss complained about the disproportionately strenuous effort it cost him to determine the sign of a square root in number theory: "many other things held me up for fewer days than this took years" and then all at once, "like a flash of lightning," he "solved the mystery." Nowadays the erratic progress characteristic of the earliest stages of development of a subject has been replaced by steady and continuous progress through the systematic construction of the theory of algebraic number fields.

The conclusion, if I am not mistaken, is that above all the modern development of pure mathematics takes place under the banner of number: the Dedekind and Kronecker definitions of the fundamental concepts of arithmetic and Cantor's general construction of the concept of number lead to an arithmeticization of function theory and serve to realise the principle that even in function theory a fact can count as proved only when in the last resort it is reduced to relations between rational integers. The arithmeticization of geometry is accomplished by the modern investigations in noneuclidean geometry in which it is a question of a strictly logical construction of the subject and the most direct possible and completely satisfactory introduction of number into geometry.

The aim of the present report is to describe the results of the theory of algebraic number fields, with their proofs, in a logical development and from a unified point of view and so to contribute towards bringing nearer the time when the achievements of our great classical authors of number theory become the common property of all mathematicians. Historical arguments and even discussions about priority have been completely avoided. To enable me to confine the description to a relatively small space I have been at pains throughout to trace the most productive sources and when a choice presented itself I have always given preference to the sharper and more widely used tools. The question of deciding which of several proofs is simplest and most natural cannot in most cases be settled in the abstract, but only after

examining whether the underlying principles can be generalised and used for further investigation do we obtain a reliable answer.

The first part of the report deals with the general theory of algebraic number fields; this theory appears to us as a mighty building supported on three foundation pillars: the theorem on unique factorisation into prime ideals, the theorem on the existence of units and the transcendental expression of the class number. The second part contains the theory of Galois number fields in which also the laws of general field theory are included. The third part is dedicated to the classical example of quadratic fields. The fourth part deals with cyclotomic fields. Finally the fifth part develops the theory of those fields which Kummer took as a basis for his researches into higher reciprocity laws and which on this account I have named after him. It is clear that the theory of these Kummer fields represents the highest peak reached on the mountain of today's knowledge of arithmetic; from it we look out on the wide panorama of the whole explored domain since almost all essential ideas and concepts of field theory, at least in a special setting, find an application in the proof of the higher reciprocity laws. I have tried to avoid Kummer's elaborate computational machinery, so that here too Riemann's principle may be realised and the proofs completed not by calculations but purely by ideas.

The theories treated in the third, fourth and fifth parts are all theories of particular abelian or relatively abelian fields. A further example of such a theory is the complex multiplication of elliptic functions, in that we understand this as a theory of those number fields which are abelian extensions of a given imaginary quadratic field. Studies of complex multiplication must, however, be denied inclusion in the present report since the results of this theory have not yet been worked out to such a level of simplicity and completeness that a satisfactory description can be given at present.

The theory of number fields is a structure of wonderful beauty and harmony; the most richly endowed part of this structure seems to me to be the theory of abelian and relatively abelian fields which Kummer by his work on the higher reciprocity laws and Kronecker by his studies in complex multiplication and elliptic functions have revealed to us. The deep insight into this theory which the work of these two mathematicians gives us shows us at the same time that in this field of knowledge an abundance of precious treasures still lies concealed, offering a rich reward for the scholar who knows the value of such gems and who lovingly applies the skill to win them.

The five parts of the report which we described above are divided into chapters and sections, and in these we always state the theorems and lemmas first and follow them with their proofs. I think of the reader as a traveller: the lemmas are wayside halts; the theorems are larger stations signalled in advance so that the activity of the mind can rest there. Those theorems which according to their fundamental significance are main destinations or which appear suitably outstanding as departure points for further advances into as

yet undiscovered country are displayed in italics[1]; these are Theorems 7, 31, 40, 44, 45, 47, 56, 82, 94, 100, 101, 131, 143, 144, 150, 158, 159, 161, 164, 166, 167.

My friend Hermann Minkowski has read the proofs of this report with great care; he also read most of the manuscript. His suggestions have led to many significant improvements, both in content and presentation. For all his help I offer him my most hearty thanks.

My thanks are due also to my wife, who transcribed the whole manuscript and prepared the index.

Finally I owe grateful acknowledgement to the Editorial Committee of the Deutsche Mathematiker-Vereinigung, in particular to Mr A. Gutzmer for reading the proofs, and to the publishers George Reimer for their wide-reaching cooperation in the production of the printed version.

Göttingen, 10 April 1897 DAVID HILBERT

[1] This has not been done in the present translation in which all theorems are printed in italics.

Table of Contents

Part II. Galois Number Fields

Part III. Quadratic Number Fields

Part V. Kummer Number Fields

Introduction to the English Edition

Franz Lemmermeyer and *Norbert Schappacher*[1]

1. The Report

David Hilbert's (1862–1943) so-called *Zahlbericht* of 1897,[2] which appears here for the first time in English, was the principal textbook on algebraic number theory for a period of at least thirty years after its appearance. Emil Artin, Helmut Hasse, Erich Hecke, Hermann Weyl and many others learned their number theory from this book. Even beyond this immediate impact Hilbert's *Zahlbericht* has served as a model for many standard textbooks on algebraic number theory through the present day—cf. for instance Samuel's little book,[3] or the first chapter of Neukirch's textbook.[4] As a matter of fact, except for minor details (see Section 4 below), at least the first two parts of Hilbert's text can still today pass for an excellent introduction to classical algebraic number theory.

But even though Hilbert's presentation definitely left its mark on this material, the text does remain a *Bericht*, i.e., a report, commissioned as it was by the *Deutsche Mathematiker-Vereinigung* (D.M.V., the German Mathematical Society), on the state of the theory around 1895. During the first years of its existence, the commissioning of comprehensive reports on all parts of mathematics was an important part of the activities of the D.M.V. The first ten volumes of the *Jahresbericht* contain thirteen such reports. David Hilbert and Hermann Minkowski were asked to write a joint report covering all of number theory. Eventually Hilbert and Minkowski decided to split the report, and it was agreed that Minkowski's part should cover the elementary aspects of number theory like continued fractions, quadratic forms and the geometry

[1] The authors would like to thank René Schoof for helpful comments during the preparation of this introduction.

[2] D. Hilbert, *Die Theorie der algebraischen Zahlkörper*, Jahresbericht der Deutschen Mathematiker-Vereinigung 4 (1897), pp. 175–546, re-edited in D. Hilbert, *Gesammelte Abhandlungen*, vol. 1, Berlin, Heidelberg, etc.: Springer, 1932 (second edition 1970), pp. 63–363. — A French edition appeared in 1910 (in spite of its printed date): D. Hilbert, *Théorie des corps de nombres algébriques*, traduit par M.A. Lewy (professeur au lycée Voltaire), Annales de la Faculté des Sciences de l'Université de Toulouse, 1909, 3ᵉ fasc.

[3] P. Samuel, *Théorie algébrique des nombres*, Paris: Hermann, 1967.

[4] J. Neukirch, *Algebraische Zahlentheorie*, Heidelberg etc.: Springer, 1992.

of numbers. But in the end, only Hilbert's part was actually written. It is interesting to compare Hilbert's *Zahlbericht* for instance to the monumental report by A. Brill and M. Noether "on the development of the theory of algebraic functions in former and recent times,"[5] which is much more obviously historically oriented than Hilbert's *Zahlbericht*, and much less of a systematic introduction to the field. On the applied side, there was for example a report on the development and the main tasks of the theory of simple frameworks.[6]

Because it is above all a report, it is not in the *Zahlbericht* that one finds Hilbert's most important, original contributions to number theory—although it does include Hilbert's proof of the Kronecker-Weber theorem[7] as well as the theory of higher ramification groups, i.e., Hilbert's development from the early 1890s of Dedekind's arithmetic theory of Galois extensions of number fields. Indeed, Hilbert's most impressive original contribution to number theory came after the *Zahlbericht*; it was his conjectural anticipation of most of the theorems of Class Field Theory, based on a remarkably deep analysis of the arithmetic of quadratic extensions of number fields. This work appeared in two articles, in 1899 and 1902. The reader interested in this aspect of Hilbert's *œuvre* will still have to read German—see the first volume of Hilbert's *Gesammelte Abhandlungen* and Hasse's appreciation of Hilbert's number theoretical achievements therein.[8]

Coming back to the *Zahlbericht*, for Hilbert reporting on the state of algebraic number theory did not mean writing an inventory of theorems amassed in the course of the nineteenth century,[9] but rather the production of a con-

[5] A. Brill, M. Noether, *Bericht über die Entwicklung der Theorie der algebraischen Funktionen in älterer und neuerer Zeit*, Jahresbericht der Deutschen Mathematiker-Vereinigung **3** (1892–93), pp. 107–565.

[6] L. Henneberg, *Bericht über die Entwicklung und die Hauptaufgaben der Theorie der einfachen Fachwerke*, Jahresbericht der Deutschen Mathematiker-Vereinigung **3** (1892–93), pp. 567–599.

[7] For a review of early (purported) proofs of this theorem, see O. Neumann, *Two proofs of the Kronecker-Weber theorem "according to Kronecker, and Weber"*, J. Reine Angew. Math. **323** (1981), 105–126, in particular p. 125, and N. Schappacher, *On the History of Hilbert's Twelfth Problem, I: Paris 1900 – Zürich 1932: The Comedy of Errors, in: Matériaux pour l'histoire des mathématiques au XX siècle*, Actes du colloque à la mémoire de Jean Dieudonné (Nice, 1996), "Séminaires et Congrès" **3** (1998), 243–273.

[8] D. Hilbert, *Gesammelte Abhandlungen*, vol. 1, Berlin, Heidelberg, etc.: Springer, 1970. Hasse's note: "Zu Hilberts algebraisch-zahlentheoretischen Arbeiten," is on pp. 528–535.

[9] This may be what the D.M.V. had in mind, as they certainly were aware of H.J.S. Smith's report on the theory of numbers [Collected Mathematical Papers 1, 38–364] presented to the London Mathematical Society, which is an invaluable document for anyone interested in the number theory of the 19th century, but lacks the coherence of Hilbert's *Zahlbericht*. — One should also mention Paul Bachmann's work in five volumes, the fifth volume of which was already written under the influence of Hilbert's *Zahlbericht*: P. Bachmann, *Zahlentheorie, Versuch einer Gesammtdarstellung*, Leipzig: Teubner; vol. I, Die Elemente der Zahlentheorie (1892); vol. II, Die Analytische Zahlentheorie (1894); vol. III,

ceptually coherent theory, which would then also point the way to further research. It is because of this goal: to indicate, and thereby influence future directions of research, that Hilbert's undertaking is most ambitious, and most open to criticism. Such criticism is of course easy to voice today, because we can base our judgement on another one hundred years of number theoretic research. Still, it is neither futile, nor is it *a priori* unjust, to put Hilbert's text into this perspective, because the *Zahlbericht* was precisely written with the idea of steering the further development of the theory.

2. Later Criticism

Probably the most outspoken criticism of tendencies expressed in the *Zahlbericht* that has been published by an eminent number theorist is due to André Weil and concerns specifically Hilbert's treatment, in the latter parts of the work, of Kummer's arithmetic theory of the cyclotomic field of ℓ-th roots of unity, for a regular prime number ℓ. In fact, Weil's introduction to Kummer's Collected Papers begins:[10]

> The great number-theorists of the last century are a small and select group of men. ... Most of them were no sooner dead than the publication of their collected papers was undertaken and in due course brought to completion. To this there were two notable exceptions: Kummer and Eisenstein. Did one die too young and the other live too long? Were there other reasons for this neglect, more personal and idiosyncratic perhaps than scientific? Hilbert dominated German mathematics for many years after Kummer's death [in 1893]. More than half of his famous *Zahlbericht* (*viz.*, parts IV and V) is little more than an account of Kummer's number-theoretical work, with inessential improvements; but his lack of sympathy for his predecessor's mathematical style, and more specifically for his brilliant use of p-adic analysis, shows clearly through many of the somewhat grudging references to Kummer in that volume.

It seems difficult to prove—or to disprove, for that matter—Weil's suspicion that it was Hilbert's influence which prevented the timely publication of Kummer's collected papers. Hilbert and Minkowski in their correspondence

---

Die Lehre von der Kreistheilung (1872); vol. IV, Die Arithmetik der quadratischen Formen (part 1, 1898; part 2, 1923); vol. V, Allgemeine Arithmetik der Zahlkörper (1905).

[10] E.E. Kummer, *Collected Papers*, edited by André Weil, vol. 1, Heidelberg etc.: Springer, 1975, p. 1.

about the *Zahlbericht*—at a time when Minkowski was still trying to contribute his share to a more extensive report on number theory—deplore the fact (and blame the Berlin Academy for it) that Eisenstein's collected papers had not been published.[11] An analogous comment by Hilbert or Minkowski about Kummer's collected papers is not known; instead, there is direct evidence that Hilbert complained to Minkowski about how unpleasant he found it to have to work through Kummer's papers.[12] This is also evident in the *Zahlbericht*; for instance in the preface: "I have tried to avoid Kummer's elaborate computational machinery, so that here too Riemann's principle may be realized and the proofs completed not by calculations but by pure thought."[13]

Readers of the first generation, echoing Hilbert's announcement, have praised the *Zahlbericht* in particular for having simplified Kummer.[14] Thus

[11] See H. Minkowski, *Briefe an David Hilbert, mit Beiträgen und herausgegeben von L. Rüdenberg und H. Zassenhaus*, Berlin, Heidelberg, New York: Springer, 1973, p. 72, Minkowski to Hilbert 12-4-1895: "Eisensteins Werke gesammelt herauszugeben, wäre wirklich eine Pflicht und ausgeführt ein Verdienst; und für die Berliner Akademie wäre es eine ewige und wohlverdiente Schande, wenn jemand sonst dieses Unternehmen angriffe."

[12] See *loc. cit.*, p. 75f, Minkowski to Hilbert 22-1-1896: "Ich bin doch etwas zu spät an das Referat gegangen. Jetzt finde ich natürlich viele hübsche Probleme, von denen es ganz schön gewesen wäre, wenn ich sie erledigt hätte. Die Jordanschen Aufsätze sind eigentlich recht interessant. Aber wenn Dir schon die Kummerschen Rechnungen unangenehm waren, so würden die Jordanschen Operationen, sein 'pour fixer les idées' Dir einen wahren Ekel einjagen."

[13] D. Hilbert, *Gesammelte Abhandlungen*, vol. 1, Berlin, Heidelberg, etc.: Springer, 1970, p. 67 (cf. p. X of the translation below): "Ich habe versucht, den großen rechnerischen Apparat von KUMMER zu vermeiden, damit auch hier der Grundsatz von RIEMANN verwirklicht würde, demzufolge man die Beweise nicht durch Rechnungen, sondern lediglich durch Gedanken zwingen soll." The picture of Riemann that Hilbert alludes to here was central in Felix Klein's campaign to elevate Riemann beyond comparison. For instance, Klein confronted Riemann with Eisenstein, whom he called a *Formelmensch*, a man of formulas. A nice tit for tat is to be found in Carl Ludwig Siegel's article *Über Riemanns Nachlaß zur analytischen Zahlentheorie* from 1932—see C.L. Siegel, *Werke*, edited by Chandrasekharan and Maaß, New York, Berlin, etc.: Springer, vol. I, p. 276, where Siegel, after having gone through Riemann's formidable handwritten notes on the zeta function, remarks: "The legend according to which Riemann found the results of his mathematical work via 'big general' ideas, without using the formal tools of analysis, does not seem to be as widespread any more as in Klein's time."

[14] Hilbert's proofreader and friend Minkowski, however, was less enthusiastic when he read Hilbert's treatment of Kummer's theory for the first time: He found the calculations still rather "involved," and Hilbert's proof of the reciprocity law "not easy to read." — see H. Minkowski, *Briefe an D. Hilbert, mit Beiträgen und herausgegeben von L. Rüdenberg und H. Zassenhaus*, Berlin, Heidelberg, New York: Springer, 1973, p. 86: Minkowski to Hilbert 17-11-1896: "... 20 Seiten habe ich bereits durchgesehen, bis zu der Stelle [around §126?], wo die langen Rechnungen anfangen. Sie sind doch noch ziemlich verwickelt." and p. 92, Minkowski to Hilbert 31-1-1897: "Dein Beweis des Reziprozitätsgesetzes ist nicht leicht zu lesen." Minkowski's subsequent sentence indicates that this refers to the proof given in §§155–161 of the *Zahlbericht*. At this point, Minkowski may not have

Hasse in 1932 mentions Kummer's "complicated and less than transparent proofs", which Hilbert replaced by new ones.[15] In 1951, however, Hasse added an afterthought describing the two rival traditions in the history of number theory: on the one hand, there is the Gauss-Kummer tradition which aims at explicit, constructive control of the objects studied, and which was carried on in particular by Kronecker and Hensel. The Dedekind-Hilbert tradition, on the other hand, aims above all at conceptual understanding. Although less critical of the *Zahlbericht* than Weil, Hasse saw the need to plead for an "organic equilibrium" of both approaches to number theory, as opposed to the "domination" of Hilbert's approach.[16]

Emil Artin, in an address for a general audience given on the occasion of Hilbert's 100th birthday in 1962, acknowledged the "great simplification"

---

known yet that Hilbert was going to give an alternative proof in §§166–171 of the *Zahlbericht*.

[15] D. Hilbert, *Gesammelte Abhandlungen*, vol. 1, Berlin, Heidelberg, etc.: Springer, 1970, p. 529: "HILBERT gibt hier neue, von den umständlichen und wenig durchsichtigen Rechnungen KUMMERs freie Beweise."

[16] See H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Berlin: Akademie-Verlag, 1952; Reprint Berlin etc.: Springer, 1985, p. VII – VIII: "Der Sinn dafür, daß die explizite Beherrschung des Gegenstandes bis in alle Einzelheiten mit der allgemeinen Fortentwicklung der Theorie Schritt halten sollte, war bei Gauss und später vor allem noch bei Kummer in ganz ausgeprägter Weise vorhanden. ... Unter dem beherrschenden Einfluß, den Hilbert auf die weitere Entwicklung der algebraischen Zahlentheorie ausgeübt hat, ist jedoch dieser Sinn mehr und mehr verlorengegangen. Es ist typisch für Hilberts ganz auf das Allgemeine und Begriffliche, auf Existenz und Struktur gerichteten Einstellung, daß er in seinem Zahlbericht alle mit der expliziten Beherrschung des Gegenstandes sich befassenden Untersuchungen und Ergebnisse von Kummer und anderen durch kurze Hinweise oder Andeutungen abtut, ohne sich mit ihnen im einzelnen zu beschäftigen, wie er ja auch die mehr rechnerischen, konstruktiven und daher der expliziten Durchführung leicht zugänglichen Beweismethoden Kummers systematisch und folgerichtig durch mehr begriffliche, numerisch schwerer zugängliche und kaum kontrollierbare Schlußweisen ersetzt hat. Auch Dedekind mit seiner stark begrifflichen, schon tief ins Axiomatische vorstoßenden Methodik hat an dieser Entwicklung entscheidenden Anteil, während auf der andern Seite die mehr konstruktiven Methoden von Kronecker und Hensel die Kummersche Tradition weiterführen, sich aber gegenüber dem beherrschenden Einfluß Hilberts nur schwer durchsetzen, bis dann allerdings in letzter Zeit entscheidende Erfolge gerade dieser Methodik den Boden für die Rückkehr zu einem organischen Gleichgewicht beider Richtungen bereitet haben."

Zassenhaus shares Hasse's point of view in his note *Zur Vorgeschichte des Zahlberichts*, in: H. Minkowski, *Briefe an D. Hilbert, mit Beiträgen und herausgegeben von L. Rüdenberg und H. Zassenhaus*, Berlin, Heidelberg, New York: Springer, 1973, p. 17–21): "Andererseits hat D. HILBERT mit charakteristischer Energie, aber auch, historisch gesehen, mit einer gewissen Einseitigkeit praktisch die Disziplin der algebraischen Zahlkörpertheorie aus dem historisch gegebenen Material herausmodelliert."

that Hilbert achieved in presenting Kummer's results.[17] According to Olga Taussky's recollections, however, "it was only ... at Bryn Mawr, that Emmy [Noether] burst out against the *Zahlbericht*, quoting also Artin as having said that it delayed the development of algebraic number theory by decades."[18] We have no way of knowing what Emmy Noether might have had in mind when she made the remark remembered by Taussky, and we do not want to speculate on this. Let us look instead a bit more closely at Hilbert's treatment of Kummer's theory.

3. Kummer's Theory

The results of Kummer's theory which both Hilbert and Weil, in rare unison, refer to as the highest peak of Kummer's number theoretic work[19] were the general reciprocity law for ℓ-th power residues, in the case of a regular odd prime number ℓ, together with the theory of genera in a Kummer extension of $\mathbf{Q}(\zeta_\ell)$ which had to be developed along the way. Hilbert refers to both as the arithmetic theory of Kummer fields. The general reciprocity law is first dealt with in the *Zahlbericht* in §§154–165, based on Eisenstein's reciprocity law which relates a rational to an arbitrary cyclotomic integer. The reciprocity law and its *Ergänzungssätze* (complementary theorems) are stated as Satz 161. Hilbert's presentation makes sytematic use of the power residue symbol (see in particular the momentous and original Satz 150 of the *Zahlbericht*), as well as the local Hilbert symbols. At the bad places the latter are given explicitly by Kummer's logarithmic derivatives—see §131. Today we would call this an "explicit reciprocity law," in the sense of the research development

[17] E. Artin, *Collected Papers*, New York, Berlin, etc.: Springer, 1965, p. 549: Hilbert "machte durch große Vereinfachung die Ergebnisse Kummers einem größeren Leserkreis zugänglich."

[18] See *Emmy Noether, a tribute to her life and work*, edited by Brewer and Smith, M. Dekker 1981, p. 82, cf. p. 90. — Olga Taussky was one of the young mathematicians who helped with the editing of the first volume of Hilbert's *Gesammelte Abhandlungen*. She claims *loc. cit.* that Hilbert's original publications were full of errors of all kinds. But the only changes made by the editors of the collected works that we are aware of is the unfortunate replacement, in Hilbert's article *Über den Dirichlet'schen biquadratischen Zahlkörper* [Math. Ann. **45** (1894), 309–340], of the somewhat unusual abbreviation "bzglf." for "bezüglichenfalls" in Hilbert's original text, meaning "respectively," by the word "bezüglich," which means "with respect to".

[19] D. Hilbert, *Gesammelte Abhandlungen*, vol. 1, Berlin, Heidelberg, etc.: Springer, 1970, p. 66 (p. X of the translation): "Es ist die Theorie dieses Kummerschen Körpers offenbar auf der Höhe des heutigen arithmetischen Wissens die äußerste erreichte Spitze ..." — E.E. Kummer, Collected Papers, edited by André Weil, vol. 1, Heidelberg etc.: Springer, 1975, p. 9: "This is the peak he [Kummer] sighted for the first time in January 1848, and whose summit he reached ten years later."

given new impetus in the late 1920s by Artin and Hasse and which continues to the present day.[20] The product formula for the local Hilbert symbols, i.e., "Hilbert's reciprocity law," appears in this treatment almost negligently as an auxiliary result, Satz 163 in §162.

However, once Hilbert has established all of Kummer's theory, he sets out afresh, in §§166–171, to reprove all of it, but avoiding this time Kummer's explicit formulæ for the symbols at the bad places, and controlling them instead via the product theorem, by information gathered at the primes not dividing ℓ. It may have been especially this second presentation of Kummer's theory that struck readers as a simplification, or at least as a way to get rid of Kummer's computational approach. Weil's wholesale claim quoted above, to the effect that Hilbert had only "inessential improvements" to offer on Kummer's theory, does not seem to do justice to Hilbert's double attempt to come to grips with this theory, even though, of course, whether or not his presentation is seen as an improvement over Kummer may be in the mind of the beholder.

Working up towards his general reciprocity law, Kummer's central achievement was to build up genus theory for Kummer extensions of $\mathbf{Q}(\zeta_\ell)$. Accordingly, genus theory plays a very important role in the *Zahlbericht*. This is quite different from what we are used to nowadays: for instance, the books by Samuel or Neukirch cited above never even mention genus theory. One reason for its disappearance in our time was Chevalley's introduction of idèles, which made it possible to develop class field theory without going through the

---

[20] P. Furtwängler, *Die Reziprozitätsgesetze für Potenzreste mit Primzahlexponenten in algebraischen Zahlkörpern I, II, III*, Math. Ann. **67** (1909), 1–31; **72** (1912), 346–386; **74** (1913), 413–429; T. Takagi, *Über das Reziprozitätsgesetz in einem beliebigen algebraischen Zahlkörper*, J. of the College of Science Tokyo **4** (1922); Coll. Papers, 179–216; E. Artin & H. Hasse, *Die beiden Ergänzungssätze zum Reziprozitätsgesetz der l^n-ten Potenzreste im Körper der l^n-ten Einheitswurzeln*, Abh. Math. Sem. Hamburg **6** (1928), 146–142; Coll. Papers Artin (1965), 142–158; H. Hasse, *Über das Reziprozitätsgesetz der m-ten Potenzreste*, J. Reine Angew. Math. **158** (1927), 228–259; Math. Abh. I, 294–325; K. Iwasawa, *On explicit formulas for the norm residue symbol*, J. Math. Soc. Japan **20** (1968), 151–165; I. Shafarevich, *A general reciprocity law*, Am. Math. Soc. Transl. **4** (1956), 73–106; J. Coates, A. Wiles, *Explicit reciprocity laws*, Journées arithm. Caen 1976, Astérisque **41/42** (1977), 7–17; A. Wiles, *Higher reciprocity laws*, Ann. Math. **107** (1978), 235–254; A. Brückner, *Explizites Reziprozitätsgesetz und Anwendungen*, Vorlesungen aus dem Fachbereich Mathematik der Universität Essen, 1979; G. Henniart, *Sur les lois de réciprocité explicites*, J. Reine Angew. Math. **329** (1981), 177–203; B. Perrin-Riou, *Théorie d'Iwasawa des représentations p-adiques sur un corps local*, Inventiones Math. **115** (1994), 81–149; K. Kato, *General explicit reciprocity laws*; to appear in the forthcoming first volume of the Korean journal: Advanced Studies in Mathematics; as well as recent unpublished work by P. Colmez, as well as by F. Cherbonnier & P. Colmez [to appear in Journal AMS]. — With these last papers, history has come around full circle in that the "explicit" laws have themselves been absorbed into a new general abstract theory.

notorious index calculus of the ideal-theoretic approach via genus theory.[21] Let us take a closer look at how genus theory is treated in Hilbert's *Zahlbericht*.

Genus theory has changed dramatically since it was created by Gauss (who himself followed in the footsteps of Euler and Lagrange).[22] Given an extension K/k of number fields, we can define the genus class group of K as the factor group of the ideal class group of K corresponding by class field theory to the extension FK/K, where F is the maximal abelian extension of k such that FK/K is unramified. Genus theory in Hilbert's *Zahlbericht* is the special case where K/k is a Kummer extension of prime degree ℓ, with $k = \mathbf{Q}(\zeta_\ell)$ a regular cyclotomic field.

Whereas Kummer, in the tradition of Gauss and Dirichlet, used the power residue symbol to define genera,[23] Hilbert built his theory on the norm residue symbol. Using the concept of factor groups (which Hilbert is so successful in avoiding as a theoretical notion—see below), his definition[24] boils down to the following: Let ℓ be an odd prime, k be a number field containing the group μ_ℓ of ℓ-th roots of unity, assume that the class number h of k is not divisible by ℓ, and let $K = k(\sqrt[\ell]{\mu})$ be a Kummer extension of k; assume moreover that the class number h of k is not divisible by ℓ and let h^* be an integer such that $hh^* \equiv 1 \bmod \ell$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ denote the primes of k that ramify in K/k, and define a homomorphism $X : k^\times \longrightarrow \mu_\ell^t$ by the rule $\alpha \longmapsto \{(\frac{\alpha,\mu}{\mathfrak{p}_1}), \cdots, (\frac{\alpha,\mu}{\mathfrak{p}_t})\}$. Let $X(E)$ denote the image of the unit group E of $k^\times$ under X, and define the homomorphism χ from the group of invertible ideals of K to $\mu_\ell^t/X(E)$ by putting $\chi(A) = X(\alpha) \cdot X(E)$, where α is a generator of the principal ideal $N_{K/k}A^{hh^*}$. This is clearly well defined, and ideals of K having the same image under χ are said to belong to the same genus. The kernel of χ is called the principal genus. The fact that norms are norm residues implies that each genus is a collection of ideal classes.

---

[21] See for instance Hasse's Zahlbericht, I §6, p. 23–24; Ia, §10, §§12–16. — Helmut Hasse's follow-up to Hilbert's *Zahlbericht*, also called "Hasse's Zahlbericht," appeared in three parts [Part I, Jahresbericht D.M.V. **35** (1926), 1–55; part Ia, ibid. **36** (1927), 233–311; part II, Ergänzungsband **6** (1930), 1–201]. It contains a presentation of Takagi's class field theory including Artin's reciprocity law and Furtwängler's principal ideal theorem, which appeared just in time for inclusion.

[22] See e.g. G. Frei, *On the development of the genus group in number fields*, Ann. Sci. Math. Quebec **3** (1979), 5–62. For modern presentations of genus theory see the books of D. Zagier [*Zetafunktionen und quadratische Körper. Eine Einführung in die höhere Zahlentheorie*, Berlin, Heidelberg, etc.: Springer, 1981] for the quadratic and A. Fröhlich [*Central extensions, Galois groups, and ideal class groups of number fields*, AMS 1983.] for the general case.

[23] E.E. Kummer, *Über die allgemeinen Reciprocitätsgesetze der Potenzreste*, Collected Papers I, 673–687, in particular p. 678.

[24] See *Zahlbericht*, §66 and §84 for quadratic fields and equivalence in the usual and strict sense, respectively, and §150 for Kummer fields.

This definition is also valid for $\ell = 2$ and equivalence in the usual sense if one is willing to use infinite primes; these were, however, introduced by Hilbert only after his *Zahlbericht* was written.[25]

The main problem of genus theory was to find a formula for the number of genera. Traditionally, this is accomplished by proving a lower and an upper bound which are called the first and the second inequality, respectively (these are special cases of the corresponding inequalities of class field theory).

To see the connection of genus theory with the general reciprocity law, recall Gauss's second proof of the quadratic reciprocity law: Let t denote the number of distinct primes dividing the discriminant of k. Then the first inequality of genus theory says that there are at most 2^{t-1} genera, i.e., that $\# \mathrm{Cl}^+(k)/\mathrm{Cl}^+(k)^2 \leq 2^{t-1}$. Using this information, a special case of the quadratic reciprocity law can be proved as follows. Let $p \equiv 1 \bmod 4$ and q be odd primes and assume that $(p/q) = +1$. Then q splits in $k = \mathbf{Q}(\sqrt{p})$, and by the first inequality k has odd class number h. Thus $\pm q^h$ is the norm of an integer from k, and considering this equation as a congruence modulo p yields $(\pm q^h/p) = +1$; but since $(-1/p) = +1$ and h is odd, this implies $(q/p) = +1$.

Kummer's line of attack was similar (the basic idea in both proofs is the observation that norms are norm residues modulo ramified primes), but he soon found[26] that the first inequality would not suffice for a proof. In fact, Kummer's as well as Hilbert's first proof (see §160 of the *Zahlbericht*) both use that the number of genera in certain extensions is exactly ℓ. The three main differences of the proofs are:

1. Kummer's proof uses the first supplementary law, which he had derived earlier using cyclotomy,[27] whereas Hilbert can do without it.
2. Kummer works in a certain subring of the ring of integers $\mathcal{O}_K$ of the Kummer extensions K; Hilbert transfers the whole theory to $\mathcal{O}_K$.
3. Although Kummer occasionally derived necessary conditions for an integer in k to be a norm from K, the theory of the norm residue symbol is a genuine achievement of Hilbert, and it is here that he goes beyond Kummer: see e.g. Satz 167, which is a special case of Hasse's norm theorem.

[25] D. Hilbert, *Über die Theorie der relativ-Abelschen Zahlkörper*, Gesammelte Abhandlungen I, 483–509, in particular §6.

[26] "Wegen dieses Umstandes reicht auch der gefundene Satz, daß die Anzahl der wirklichen *Genera* nicht größer ist, als der λte Teil der möglichen, nicht aus, sondern es ist nöthig, daß die Anzahl der wirklichen *Genera* genau gefunden werde, wozu andere Prinzipien erforderlich sind, als welche Gauß zur Ergründung dieser wichtigen Frage für die quadratischen Formen angewendet hat." [*Über die allgemeinen Reciprocitätsgesetze der Potenzreste*, Collected Papers I, 673–687, in particular p. 682].

[27] "und zwar unter einem erheblichen Aufwande von Rechnung", as Hilbert remarks in §161.

4. A Few Noteworthy Details

Let us now look more closely at a few places where Hilbert's treatment in the *Zahlbericht* differs from what one is used to today. The first such instance occurs when Hilbert proves the unique factorization of ideals into prime ideals in the ring of integers of an algebraic number field via Leopold Kronecker's theory of forms and Dedekind's so-called "Prague Theorem"—see §§5–6.[28] Hilbert does, however, also point out alternative proofs of this key result, at the end of §6.

Since we are today looking back on the *Zahlbericht* from a distance of 100 years, a few proofs there strike us as somewhat roundabout. For instance, in the proof that precisely the prime divisors of the discriminant are ramified as well as in his discussion of the splitting of primes, in particular of those dividing the discriminant of a generating polynomial (see §§10–13 of the *Zahlbericht*), Hilbert switches again from Dedekind's ideal-theoretic language to Kronecker's theory of forms. Modern proofs built upon Hensel's p-adic theory may be more appealing.

A special feature of Hilbert's *Zahlbericht* which the unsuspecting reader may not be prepared for is the very uneven usage of notions from abstract algebra. Thus, while the notion of fields and their arithmetic is at the very heart of Hilbert's concept of algebraic number theory, and even though Hilbert uses the word "(Zahl)ring" for orders in algebraic number fields, this must not be taken as evidence that Hilbert employs here parts of our current algebraic terminology the way we would do it; rather than referring to a general algebraic structure,[29] the word "ring" is used for sets of algebraic integers which form a ring in our modern sense of the word. Similarly, but much more obviously for the modern reader, Hilbert does not have at his disposal general abstract notions from group theory that could unify the discussions of situations that we immediately recognize as analogous.[30] Most striking is the absence from the *Zahlbericht* of the notion of quotient groups.[31]

[28] For the background of this argument, see H.M. Edwards, *The Genesis of Ideal Theory*, Archive Hist. Exact Sciences **23** (1980), 321–378; here in particular: section 13, pp. 364–368.

[29] According to I. Kleiner, *From numbers to rings: the early history of ring theory*, Elem. Math. **53** (1998), 18–35, the modern axiomatic definition of a field is due to Steinitz (1910), that of a ring to Fraenkel (1914) and Sono (1917).

[30] This omission seems to be deliberate: in his letter from 21-7-1896 (loc. cit.), Minkowski suggested that the inclusion of a few lemmas on Abelian groups in §100 would allow the reader to enjoy Hilbert's proof of the theorem of Kronecker-Weber without distractions ["Damit der Leser zu einem völlig ungestörten Genusse desselben komme, möchte ich empfehlen, die gebrauchten Hilfssätze über Abelsche Gruppen mit Andeutungen ihrer Beweise vorweg in §100 zu absolviren."]

[31] Factor groups were first defined by O. Hölder, *Zurückführung einer algebraischen Gleichung auf eine Kette von Gleichungen*, Math. Ann. **34** (1889), 26–56; they

Thus, when we would say that "G/H is cyclic of order h," Hilbert has to write elaborate prose: "the members of G are each obtained precisely once when we multiply the members of H by $1, g, \ldots, g^{h-1}$ where g is a suitably chosen member of G"(see e.g. *Zahlbericht*, Sätze 69, 71 and 75).

Contrary to these points, which, from our vantage point, may be considered as shortcomings, but which the *Zahlbericht* shares with most other texts on the subject before Hecke's book from 1923, some other unusual features of the text have to be counted among its pearls. In fact, theorems 89–94 may be regarded as the first highlight of the *Zahlbericht*. Here Hilbert *did* "point the way to further research."

Hilbert's Satz 89 says that the ideal class group is generated by the classes of prime ideals of degree 1. In the special case of cyclotomic fields, this result is due to Kummer.[32] It is a very special case of the density theorems of class field theory, such as Chebotarev's, but it is accessible without analytic methods. Already Max Deuring[33] remarked that this theorem has been somewhat neglected. This is also demonstrated by the fact that Hilbert's proof of this theorem has not been simplified in 100 years. Even worse: it was only in 1987 that Lawrence Washington[34] noticed a gap in it — which is, however, easy to fix.

Hilbert's Satz 90. Again it was Kummer[35] who discovered (in the special case of Kummer extensions of $\mathbf{Q}(\zeta_p)$) what is probably the most famous theorem from the *Zahlbericht*. It is hardly necessary today to recall that E. Noether generalized Satz 90 considerably; in cohomological formulation, her result reads $H^1(G, K^\times) = 1$, where K/k is a normal extension of number fields

are discussed in Weber's *Algebra 2*, Braunschweig 1896, but authors ranging all the way from Heinrich Weber himself (*Ueber Zahlengruppen in algebraischen Körpern*, Math. Ann. **48** (1897), 433–473) to Erich Hecke (*Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig 1923, where Chapters II and III are devoted to Abelian groups) found it necessary to explain to their readers the concept of groups in general, and of factor groups in particular. — See L. Corry, *Modern algebra and the rise of mathematical structures*; Science Networks, vol 17, Basel, Boston (Birkhäuser) 1996, in particular Chapter III, for an extensive discussion of Hilbert's position in the development of modern abstract algebra.

[32] E.E. Kummer, *Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfaktoren*, Collected Papers I, 211–251, in particular pp. 241–243.

[33] In M. Deuring, *Neuer Beweis des Bauerschen Satzes*, J. Reine Angew. Math. 173 (1935), 1–4, one reads in reference to Satz 89: "...ist eine naturgemäße Verallgemeinerung eines wenig beachteten Satzes in Hilbert's *Zahlbericht*."

[34] L.C. Washington, *Stickelberger's theorem for cyclotomic fields, in the spirit of Kummer and Thaine*, Théorie des nombres, Quebec, Canada 1987, 990–993 (1989).

[35] E.E. Kummer, *Über eine besondere Art, aus complexen Einheiten gebildeter Ausdrücke*, Collected Papers I, 552–572; in particular p. 553, and *Über die allgemeinen Reciprocitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist*, Collected Papers I, 699–839; in particular p. 754.

with Galois group G. Satz 90 is the statement $\widehat{H}^{-1}(G, K^{\times}) = 1$ for cyclic G which follows from $\widehat{H}^{1}(G, K^{\times}) = 1$ using the periodicity of Tate's cohomology groups for cyclic G.

Hilbert's Satz 91 on the existence of relative units was to be the first in a series of generalizations of Dirichlet's unit theorem.[36] A similar result had been proved by Kummer[37] in a slightly different form. The theorem is contained implicitly in the index computations in Hasse's Zahlbericht (Ia, §12; Fußnote 25).

Hilbert's Satz 92. Once more, this is a result which was inspired by work of Kummer.[38] In cohomological form, the statement reads $H^{-1}(G, E_K) \neq 1$ (here K/k is a cyclic extension of prime order p and Galois group G). Today this is part of the standard theorems in class field theory known as the "Herbrand index of the unit group", which says that in fact $\# \widehat{H}^{-1}(G, E_K) = p \cdot (E_k : NE_K)$ for cyclic extensions of number fields that are unramified everywhere.

Hilbert's Satz 94. This is a forerunner of the principal ideal theorem of class field theory. It does not, however, contain Satz 94 as a special case. In contrast to Theorems 89–92, Satz 94 cannot be traced back to Kummer. In fact, it is very likely that Kummer did not even think about the possibility of ideal classes becoming principal in extensions: his invalid proof [39] that the class number of cyclotomic fields is divisible by the class number of any subfield is based on the implicit assumption that ideals do not capitulate.

It seems that the phenomenon of capitulation was discovered by Kronecker in connection with his investigations of his Jugendtraum: Kronecker[40] noticed

[36] See for instance J. Herbrand, *Sur les unités d'un corps algébrique*, C. R. Acad. Sci. Paris **192** (1931), 24–27; and E. Artin, *Über Einheiten relativ galoisscher Zahlkörper*, J. Reine Angew. Math. **167** (1932), 153–156.

[37] E.E. Kummer, *Über die allgemeinen Reciprocitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist*, Collected Papers I, 699–839; in particular pp. 785–792.

[38] E.E. Kummer, *Zwei neue Beweise der allgemeinen Reciprocitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist*, Collected Papers I, 842–882.

[39] E.E. Kummer, *Bestimmung der Anzahl nichtäquivalenter Klassen für die aus λten Wurzeln der Einheit gebildeten complexen Zahlen und die idealen Factoren derselben*, Collected Papers I, 299–322; in particular, p. 320–322. Weil remarks in this connection (ibid, p. 955): "In other contexts, of course, he had many examples of non-principal ideals in a given field which become principal in some bigger field." What Weil has in mind here is probably Kummer's observation on p. 209 of the article *Zur Theorie der komplexen Zahlen*, Collected Papers I, 203–210: "Ich bemerke nur noch, daß sie [die idealen Zahlen] ... immer die Form $\sqrt[h]{(\Phi(\alpha))}$ annehmen, wo $\Phi(\alpha)$ eine wirkliche complexe Zahl ist, und h eine ganze Zahl." Of course this can be read as "every ideal $\mathfrak{a}$ of k becomes principal in the extension $k(\sqrt[h]{\mu})$, where $\mathfrak{a}^h = (\mu)$," but one may want to be careful about assuming that this was Kummer's way of seeing things.

[40] L. Kronecker, *Ueber die Potenzreste gewisser complexer Zahlen*, Monatsber. Berlin (1880), 404–407; Werke II, 95–101.

that $k = \mathbf{Q}(\sqrt{-31})$ admitted an unramified cyclic cubic extension K in which every ideal is principal and remarked, referring to the splitting behaviour of prime ideals of k in this extension, that "it is exactly this fact which contains a clear hint at the future development in the theory of power residues, in particular for the cases excluded in Kummer's investigations."[41]

Hilbert's remarks after the proof of Satz 94 are quite mysterious: we do not know what to make of his claim that the results of Satz 94 can easily be extended to relatively abelian extensions with relative different 1 whose degree is not necessarily a prime. It is easy to make his proof work for cyclic extensions of prime power degree, and an elementary argument shows that Satz 94 then holds for cyclic extensions of arbitrary degree. But there are problems even with extensions K/k of type (p,p): of course the statement that there is a nonprincipal ideal in k that becomes principal in K continues to hold, but the claim that the class number of k is divisible by p^2 does not follow easily.[42] In fact, the correct generalization of Satz 94, namely the claim that in unramified abelian extensions K/k there are at least $(K : k)$ ideal classes that become principal, was only proved in 1991 by reduction to a group theoretic problem via Artin's reciprocity law.[43] Incidentally, Kronecker in his earlier writings used the word 'Abelian' for what is called 'cyclic' today.

Stickelberger's Theorem (Satz 138) gives the prime ideal decomposition of Gauss sums; its treatment in Hilbert's *Zahlbericht* is remarkable in two ways: first, Hilbert does not state (let alone prove) Stickelberger's theorem at all, but is content with the special case[44] already known to Jacobi and Kummer. In fact, he does not even mention Stickelberger's article in this connection although he lists it in his references. The reasons for this omission are not clear; one may speculate that Hilbert had read Stickelberger's article only superficially.

In 1933, while working on their paper on the congruence zeta function, in particular of Fermat curves, Hasse and Davenport proved a general version of the result due to Jacobi and Kummer. In February 1934, Davenport then

[41] *loc. cit.*, p. 101: "Es ist genau dieser Umstand, welcher einen deutlichen Hinweis auf die Weiterentwicklung der Theorie der Potenzreste namentlich auch für die in den Kummerschen Untersuchungen ausgeschlossenen Fälle enthält."

[42] P. Furtwängler could prove Satz 94 for unramified extensions of type (p,p) in *Über das Verhalten der Ideale des Grundkörpers im Klassenkörper*, Monatsh. Math. Phys. **27** (1916), 1–15, and a cohomological proof for the more general case (p^n,p) can be found e.g. in R. Bond, *Unramified abelian extensions of number fields*, J. Number Theory **30** (1988), 1–10.

[43] See H. Suzuki, *A generalization of Hilbert's theorem 94*, Nagoya Math. J. 121 (1991), 161–169; for more on capitulation, see K. Miyake, *Algebraic investigations of Hilbert's Theorem 94, the principal ideal theorem, and the capitulation problem*, Expos. Math. **7** (1989), 289–346.

[44] This is actually the only place in the *Zahlbericht* that we are aware of where Hilbert does not go to the borders of what was known.

discovered this generalization in Stickelberger's paper, and Hasse[45] promptly blamed Hilbert for not including it in the *Zahlbericht*. This episode indicates how much the generation of number theorists after Hilbert relied on the *Zahlbericht* as a comprehensive reference for the subject.

The second observation concerning Hilbert's approach to Stickelberger's theorem is that he ties it in with his study of normal integral bases (simply called 'normal bases' by Hilbert). A normal basis of a normal extension $k/\mathbf{Q}$ is an integral basis of the form $\{t\nu : t \in \mathrm{Gal}(K/\mathbf{Q})\}$ for some integral $\nu \in k$ (see §105). For fields k of prime degree ℓ Hilbert associates to each such normal basis a "root number" $\Omega = \nu + \zeta \cdot t\nu + \dots \zeta^{l-1} \cdot t^{l-1}\nu$, where ζ is a primitive ℓth root of unity (see §106). Satz 133 and Satz 134 characterize root numbers by four properties,[46] and Satz 135 gives the prime ideal factorization of root numbers up to conjugacy. In the special case where the normal basis is generated by Gaussian periods, the root number is a Gauss sum ("Lagrangian root number" in Hilbert's terminology).[47]

None of these results related to Stickelberger's theorem made it into the list of theorems that Hilbert considered to be "departure points for further advances" (see the Preface to the *Zahlbericht*), and at first history seemed to agree with Hilbert. In fact, after the contributions of Andreas Speiser and Emmy Noether,[48] the topic of normal integral bases lay dormant for 40 years. Then, however, things changed dramatically; for a description of the activities during the 1970s, the reader may consult Section I §1 in Albrecht Fröhlich's book.[49] Research in this area is continuing vigorously at the moment.

We hope that the special features of Hilbert's *Zahlbericht* justify this first English edition of it, and will enable it to hold its own as a classical text that readers will be happy to consult along with the many excellent textbooks on algebraic number theory which are available today, 100 years after the *Zahlbericht* was written.

---

[45] Hasse to Davenport, 22-2-1934: "Moreover the old proof and the whole matter seems to have slipped from the minds of our generation, presumably owing to Hilbert's inconceivable not giving it in his Zahlbericht." We thank Peter Roquette for this information. The letters from Hasse to Davenport are kept in Trinity College, Cambridge, UK.

[46] The fourth property, namely that ω is not an ℓth power in k, should be added to Satz 133; it follows at once from $\zeta \cdot t\Omega = \Omega$.

[47] Cf. A. Weil's ironical remarks in *La cyclotomie jadis et naguère*, Sém. Bourbaki 1973/74, no. 452 (juin 1974), Springer Lecture Notes Math. **431**, or *Œuvres scientifiques* **3** (1980), 311–328.

[48] A. Speiser, *Gruppendeterminante und Körperdiskriminante*, Math. Annalen **77** (1916), 546–562; E. Noether, *Normalbasis bei Körpern ohne höhere Verzweigung*, J. Reine Angew. Math. **167** (1932), 147–152.

[49] A. Fröhlich, *Galois module structure of algebraic integers*, Berlin, Heidelberg, etc.: Springer, 1983.

Part I

The Theory of General Number Fields

1. Algebraic Numbers and Number Fields

§1. Number Fields and Their Conjugates

A number α is called an *algebraic number* if it satisfies an equation of degree m of the form

$$\alpha^m + a_1\alpha^{m-1} + a_2\alpha^{m-2} + \cdots + a_m = 0$$

where $a_1, a_2, \ldots, a_m$ are rational numbers.

Let $\alpha, \beta, \ldots, \kappa$ be a finite number of arbitrary algebraic numbers; then the collection of all rational functions of $\alpha, \beta, \ldots, \kappa$ with integer coefficients forms a closed system of algebraic numbers which is called a *number field*, *field* or *domain of rationality* (*Dedekind* (1, 2), *Kronecker* (16)). Since in particular the sum, difference, product and quotient of two numbers of a field are also numbers of the field, it follows that a field is invariant under the four arithmetic operations of addition, subtraction, multiplication and division.

Theorem 1. *In every field k there is a number ϑ such that all other numbers of the field are polynomials in ϑ with rational coefficients.*

The degree m of the equation with rational coefficients of lowest degree satisfied by such a number ϑ is called the *degree* of the field k. The number ϑ will be called a *generator* of the field. The equation of degree m satisfied by ϑ is irreducible over the field of rational numbers. Conversely, each root of such an irreducible equation generates a number field of degree m. Let $\vartheta', \vartheta'', \ldots, \vartheta^{(m-1)}$ be the other $(m-1)$ roots of the equation; we call the fields $k', k'', \ldots, k^{(m-1)}$ generated by $\vartheta', \vartheta'', \ldots, \vartheta^{(m-1)}$ the *conjugate fields* of k. If α is any number in the field k and

$$\alpha = c_1 + c_2\vartheta + \cdots + c_m\vartheta^{m-1}$$

where $c_1, c_2, \ldots, c_m$ are rational numbers, then the numbers

$$\alpha' = c_1 + c_2\vartheta' + \cdots + c_m(\vartheta')^{m-1}$$
$$\cdots\cdots\cdots$$
$$\alpha^{(m-1)} = c_1 + c_2\vartheta^{(m-1)} + \cdots + c_m(\vartheta^{(m-1)})^{m-1}$$

which are obtained from α by means of the substitutions $t' = (\vartheta : \vartheta'), \ldots, t^{(m-1)} = (\vartheta : \vartheta^{(m-1)})$ respectively are called the numbers *conjugate* to α.

§2. Algebraic Integers

An algebraic number α is called an *algebraic integer*, or briefly an *integer*, if it satisfies an equation of the form

$$\alpha^m + a_1\alpha^{m-1} + a_2\alpha^{m-2} + \cdots + a_m = 0$$

where the coefficients $a_1, a_2, \ldots, a_m$ are all rational integers.

Theorem 2. *Every polynomial expression F in arbitrarily many algebraic integers $\alpha, \beta, \ldots, \kappa$ with integer coefficients is again an algebraic integer.*

Proof. We denote by $\alpha', \alpha'', \ldots, \beta', \beta'', \ldots, \kappa', \kappa'', \ldots$ the numbers conjugate to $\alpha, \beta, \ldots, \kappa$ respectively and form all expressions of the form

$$F(\alpha, \beta, \ldots, \kappa), F(\alpha', \beta, \ldots, \kappa), F(\alpha, \beta', \ldots, \kappa), \ldots,$$
$$\ldots, F(\alpha, \beta, \ldots, \kappa'), \ldots, F(\alpha', \beta', \ldots, \kappa), \ldots$$

The well-known theorem on symmetric functions then shows that all the coefficients of the equation satisfied by all these expressions are integers, while the coefficient of the highest power of the unknown is 1.

In particular, the sum, difference and product of two integers are again integers. Thus the property of integrality is preserved under the three operations of addition, subtraction and multiplication. An integer γ is said to be *divisible* by an integer α if there exists an integer β such that $\gamma = \alpha\beta$.

Theorem 3. *The roots of an equation of arbitrary degree r of the form*

$$\alpha^r + a_1\alpha^{r-1} + a_2\alpha^{r-2} + \cdots + a_r = 0$$

with algebraic integer coefficients $a_1, a_2, \ldots, a_r$ are algebraic integers.

Theorem 4. *When an algebraic integer α is also rational then it is a rational integer.*

Proof. Suppose $\alpha = a/b$ where a and b are rational integers relatively prime to one another and $b > 1$. If α were to satisfy an equation whose coefficients $a_1, a_2, \ldots, a_m$ are rational integers then, on multiplying this equation by b^{m-1}, we would obtain

$$\frac{a^m}{b} = -a_1 a^{m-1} - a_2 a^{m-2} b - \cdots - a_m b^{m-1} = A$$

where A is a rational integer, and this is impossible (*Dedekind* (1), *Kronecker* (16)).

§3. Norm, Different and Discriminant of a Number. Basis of a Number Field

Let α be a number in the field k; let $\alpha', \ldots, \alpha^{(m-1)}$ be the conjugates of α. Then the product

$$n(\alpha) = \alpha\alpha' \cdots \alpha^{(m-1)}$$

is called the *norm of the number* α. The norm of a number α is always a rational number. The product

$$\delta(\alpha) = (\alpha - \alpha')(\alpha - \alpha'') \cdots (\alpha - \alpha^{(m-1)})$$

is called the *different of the number* α. The different of a number in the field k is again a number in k. When we write for short

$$f(x) = (x - \alpha)(x - \alpha') \cdots (x - \alpha^{(m-1)})$$

we have

$$\delta(\alpha) = \left[\frac{df(x)}{dx}\right]_{x=\alpha}.$$

Finally the product

$$\begin{aligned} d(\alpha) &= (\alpha - \alpha')^2(\alpha - \alpha'')^2 \cdots (\alpha' - \alpha'')^2 \cdots (\alpha^{(m-2)} - \alpha^{(m-1)})^2 \\ &= \begin{vmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{m-1} \\ 1 & \alpha' & (\alpha')^2 & \cdots & (\alpha')^{m-1} \\ & & \cdots\cdots\cdots & & \\ 1 & \alpha^{(m-1)} & (\alpha^{(m-1)})^2 & \cdots & (\alpha^{(m-1)})^{m-1} \end{vmatrix}^2 \end{aligned}$$

is called the *discriminant of the number* α. The discriminant of a number is a rational number, and up to its sign it is equal to the norm of the different; we have in fact $d(\alpha) = (-1)^{m(m-1)/2} n(\delta(\alpha))$.

If α is a generator of the field its different and discriminant are nonzero. Conversely, when the different and discriminant of a number are nonzero it generates the field. If α is an algebraic integer then its norm, different and discriminant are also integers.

Theorem 5. *In a number field of degree m there always exist m integers* $\omega_1, \omega_2, \dots, \omega_m$ *with the property that every other integer* ω *of the field can be represented in the form*

$$\omega = a_1\omega_1 + a_2\omega_2 + \cdots + a_m\omega_m$$

where $a_1, a_2, \dots, a_m$ *are rational integers.*

Proof. Let α be a generator of the field. Then every number ω can be represented in the form

$$\omega = r_1 + r_2\alpha + \cdots + r_m\alpha^{m-1}$$

where $r_1, r_2, \dots, r_m$ are rational numbers. Passing to the conjugates of ω we obtain

$$\omega' = r_1 + r_2\alpha' + \cdots + r_m(\alpha')^{m-1},$$

$$\cdots\cdots\cdots$$

$$\omega^{(m-1)} = r_1 + r_2\alpha^{(m-1)} + \cdots + r_m(\alpha^{(m-1)})^{m-1};$$

and hence (in an easily understood abbreviated notation) we have, for $s = 1, 2, \dots, m$,

$$\begin{aligned} r_s &= \frac{|1, \alpha, \dots, \omega, \dots, \alpha^{m-1}|}{|1, \alpha, \dots, \alpha^{s-1}, \dots, \alpha^{m-1}|} \\ &= \frac{|1, \alpha, \dots, \omega, \dots, \alpha^{m-1}||1, \alpha, \dots, \alpha^{s-1}, \dots, \alpha^{m-1}|}{|1, \alpha, \dots, \alpha^{s-1}, \dots, \alpha^{m-1}|^2} \\ &= \frac{A_s}{d(\alpha)}, \end{aligned}$$

where A_s, being an integer polynomial function of $\alpha, \alpha', \dots, \alpha^{(m-1)}$ and $\omega, \omega', \dots, \omega^{(m-1)}$, is an integer. On the other hand A_s is equal to the rational number $r_s d(\alpha)$ and hence, by Theorem 4, A_s is a rational integer. Thus every integer ω can be expressed in the form

$$\omega = \frac{A_1 + A_2\alpha + \cdots + A_m\alpha^{m-1}}{d(\alpha)} \tag{1.1}$$

where $A_1, A_2, \dots, A_m$ are rational integers and $d(\alpha)$ is the discriminant of the generator α.

Now let s be any of the numbers $1, 2, \ldots, m$; we consider all the integers of the field expressible in the form

$$\begin{aligned}
\omega_s &= \frac{O_1 + O_2\alpha + \cdots + O_s\alpha^{s-1}}{d(\alpha)} \\
\omega_s^{(1)} &= \frac{O_1^{(1)} + O_2^{(1)}\alpha + \cdots + O_s^{(1)}\alpha^{s-1}}{d(\alpha)} \\
\omega_s^{(2)} &= \frac{O_1^{(2)} + O_2^{(2)}\alpha + \cdots + O_s^{(2)}\alpha^{s-1}}{d(\alpha)} \\
&\cdots\cdots\cdots
\end{aligned}$$

where the coefficients O, $O^{(1)}$, $O^{(2)}$, ... are all rational integers. We may suppose that O_s is nonzero and is the greatest common divisor of all the numbers O_s, $O_s^{(1)}$, $O_s^{(2)}$, ... Then the m numbers $\omega_1, \omega_2, \ldots, \omega_m$ form a set with the desired property. Namely, let ω be any integer, expressed in the form (1.1); then, according to the defining condition for ω_m, we must have $A_m = a_m O_m$ where a_m is a certain rational integer. Then, however, the difference $\omega^* = \omega - a_m\omega_m$ has the form

$$\omega^* = \frac{A_1^* + A_2^*\alpha + \cdots + A_{m-1}^*\alpha^{m-2}}{d(\alpha)}.$$

Here now we must have $A_{m-1}^* = a_{m-1}O_{m-1}$; consideration of the difference $\omega^{**} = \omega^* - a_{m-1}\omega_{m-1}$ and repetition of the procedure leads to the result of Theorem 5.

The numbers $\omega_1, \ldots, \omega_m$ are called a *basis* for the set of all integers of the field k or, briefly, a *basis for the field* k. Every other basis $\omega_1^*, \ldots, \omega_m^*$ of the field is given by formulæ of the type

$$\begin{aligned}
\omega_1^* &= a_{11}\omega_1 + \cdots + a_{1m}\omega_m \\
&\cdots\cdots\cdots \\
\omega_m^* &= a_{m1}\omega_1 + \cdots + a_{mm}\omega_m
\end{aligned}$$

where the determinant of the integral coefficients a is ± 1 (*Dedekind* (1), *Kronecker* (16)).

2. Ideals of Number Fields

§4. Multiplication and Divisibility of Ideals. Prime Ideals

The first important problem in the theory of number fields is the formulation of the laws concerning the factorisation of algebraic integers. These laws have a wonderful beauty and simplicity, exhibiting a precise analogy with the elementary laws of factorisation in the theory of rational integers and having the same fundamental importance. They were first discovered by Kummer for the special case of cyclotomic fields (*Kummer* (5,6)); their investigation for general number fields is due to Dedekind and Kronecker. The fundamental ideas of the theory are as follows.

An *ideal* $\mathfrak{a}$ in a field k is a set of infinitely many algebraic integers $\alpha_1, \alpha_2, \ldots$ with the property that every linear combination $\lambda_1\alpha_1 + \lambda_2\alpha_2 + \cdots$ (in which $\lambda_1, \lambda_2, \ldots$ are algebraic integers in k) again belongs to the set $\mathfrak{a}$.

Theorem 6. *In each ideal $\mathfrak{a}$ there exist m numbers $\iota_1, \ldots, \iota_m$ such that every other number in the ideal can be expressed as a linear combination of the form*

$$l_1\iota_1 + \cdots + l_m\iota_m$$

where $l_1, \ldots, l_m$ are rational integers.

Proof. Let s be any of the numbers $1, 2, \ldots, m$; consider all the numbers of the ideal of the form

$$\begin{aligned} \iota_s &= J_1\omega_1 + \cdots + J_s\omega_s, \\ \iota_s^{(1)} &= J_1^{(1)}\omega_1 + \cdots + J_s^{(1)}\omega_s, \\ &\quad \cdots\cdots\cdots \end{aligned}$$

where $J, J^{(1)}, \ldots$ are rational integers. We suppose that J_s is nonzero and is the greatest common divisor of all the numbers $J_s, J_s^{(1)}, \ldots$. It then follows, as in the proof of Theorem 5, that the m numbers $\iota_1, \ldots, \iota_m$ have the desired property.

The numbers $\iota_1, \ldots, \iota_m$ are said to form a *basis of the ideal* $\mathfrak{a}$. Every other basis $\iota_1^*, \ldots, \iota_m^*$ of the ideal is given by formulæ of the type

$$\begin{aligned} \iota_1^* &= a_{11}\iota_1 + \cdots + a_{1m}\iota_m \\ &\cdots\cdots\cdots \\ \iota_m^* &= a_{m1}\iota_1 + \cdots + a_{mm}\iota_m \end{aligned}$$

where the determinant of the integral coefficients a is ± 1.

If $\alpha_1, \ldots, \alpha_r$ are any r numbers of the ideal $\mathfrak{a}$ such that every number in the ideal can be expressed as a linear combination of $\alpha_1, \ldots, \alpha_r$ with coefficients which are algebraic integers of k, we write

$$\mathfrak{a} = (\alpha_1, \ldots, \alpha_r).$$

If $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$ and $\mathfrak{b} = (\beta_1, \ldots, \beta_s)$ are two ideals then the ideal formed by taking all linear combinations of $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s$ is denoted by $(\mathfrak{a}, \mathfrak{b})$, i.e. we write

$$(\mathfrak{a}, \mathfrak{b}) = (\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s).$$

An ideal which consists precisely of all the numbers of the form $\lambda\alpha$, where α is a fixed nonzero integer of the field and λ is an arbitrary integer of the field, is called a *principal ideal* and is denoted by (α), or briefly by α when there is no risk of confusion with the number α.

Each number α of an ideal $\mathfrak{a}$ is said to be *congruent to* 0 *modulo* $\mathfrak{a}$; we denote this by

$$\alpha \equiv 0 \pmod{\mathfrak{a}}.$$

If the difference of two numbers α and β is congruent to 0 modulo $\mathfrak{a}$ we say that α and β are *congruent* to one another modulo $\mathfrak{a}$ and we write

$$\alpha \equiv \beta \pmod{\mathfrak{a}};$$

otherwise they are said to be *incongruent* to one another and we write

$$\alpha \not\equiv \beta \pmod{\mathfrak{a}}.$$

If we multiply each number of an ideal $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$ by every number of a second ideal $\mathfrak{b} = (\beta_1, \ldots, \beta_s)$ and form all linear combinations of the products with algebraic integer coefficients from the field, the new ideal so obtained is called the *product* $\mathfrak{ab}$ of the two ideals $\mathfrak{a}$ and $\mathfrak{b}$; thus

$$\mathfrak{ab} = (\alpha_1\beta_1, \ldots, \alpha_r\beta_1, \ldots, \alpha_1\beta_s, \ldots, \alpha_r\beta_s).$$

An ideal $\mathfrak{c}$ is said to be *divisible* by an ideal $\mathfrak{a}$ if there exists an ideal $\mathfrak{b}$ such that $\mathfrak{c} = \mathfrak{ab}$. If an ideal $\mathfrak{c}$ is divisible by the ideal $\mathfrak{a}$ then all the numbers of $\mathfrak{c}$ are congruent to 0 modulo $\mathfrak{a}$. We have the following result concerning the divisors of an ideal.

Lemma 1. *An ideal* $\mathfrak{i}$ *is divisible by only a finite number of ideals.*

Proof. Let ι be an arbitrary nonzero number in the ideal $\mathfrak{i}$; let n be the norm of ι. If $\mathfrak{a}$ is any divisor of the ideal $\mathfrak{i}$ then the rational integer n is obviously congruent to 0 modulo $\mathfrak{a}$. Let

$$\alpha_1 = a_{11}\omega_1 + \cdots + a_{1m}\omega_m,\ \ldots,\ \alpha_m = a_{m1}\omega_1 + \cdots + a_{mm}\omega_m$$

be a basis for $\mathfrak{a}$, where $a_{11}, \ldots, a_{mm}$ are rational integers. Let $a'_{11}, \ldots, a'_{mm}$ be the smallest positive residues of $a_{11}, \ldots, a_{mm}$ respectively modulo n. Then

$$\begin{aligned} \mathfrak{a} &= (a_{11}\omega_1 + \cdots + a_{1m}\omega_m, \ldots, a_{m1}\omega_1 + \cdots + a_{mm}\omega_m) \\ &= (a'_{11}\omega_1 + \cdots + a'_{1m}\omega_m, \ldots, a'_{m1}\omega_1 + \cdots + a'_{mm}\omega_m, n) \end{aligned}$$

and this latter representation of the ideal divisor $\mathfrak{a}$ leads immediately to the assertion of the lemma.

An ideal distinct from 1 which is divisible by no ideal other than itself and the ideal 1 is called a *prime ideal.* Two ideals are called *relatively prime to* one another when they have no common ideal divisor other than 1. Two integers α and β or an integer α and an ideal $\mathfrak{a}$ are said to be *prime* to one another when the principal ideals (α) and (β) or the principal ideal (α) and the ideal $\mathfrak{a}$ respectively are prime to one another (*Dedekind* (1)).

§5. Unique Factorisation of an Ideal into Prime Ideals

We have the following fundamental result.

Theorem 7. *Every ideal* $\mathfrak{i}$ *can be represented in one and only one way as a product of prime ideals.*

Dedekind has recently given a new exposition of his proof (*Dedekind* (1)). The method of proof followed by Kronecker is based on his theory of the algebraic forms belonging to a number field. The significance of this theory of forms becomes clearer if we first derive the theorems of ideal theory directly; for this purpose the following lemma plays an essential part.

Lemma 2. *If the coefficients $\alpha_1, \alpha_2, \ldots, \beta_1, \beta_2, \ldots$ of two polynomials in one variable*

$$F(x) = \alpha_1 x^r + \alpha_2 x^{r-1} + \cdots,$$

$$G(x) = \beta_1 x^s + \beta_2 x^{s-1} + \cdots$$

are algebraic integers and the coefficients $\gamma_1, \gamma_2, \ldots$ of the product

$$F(x)G(x) = \gamma_1 x^{r+s} + \gamma_2 x^{r+s-1} + \cdots$$

are all divisible by the integer ω then each of the numbers $\alpha_1\beta_1, \alpha_1\beta_2, \ldots, \alpha_2\beta_1, \alpha_2\beta_2, \ldots$ is also divisible by ω (Kronecker (19), Dedekind (7), Mertens (1), Hurwitz (1, 2)).

From this lemma we obtain easily the following sequence of theorems (*Hurwitz* (1)).

Theorem 8. *Corresponding to each ideal $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$ we can find an ideal $\mathfrak{b}$ such that the product $\mathfrak{ab}$ is a principal ideal.*

Proof. We set

$$F(x) = \alpha_1 x^r + \alpha_2 x^{r-1} + \cdots$$

and

$$F^{(i)}(x) = \alpha_1^{(i)} x^r + \alpha_2^{(i)} x^{r-1} + \cdots \qquad (i = 1, \ldots, m-1),$$

where the $\alpha_k^{(i)}$ are the numbers conjugate to α_k; we form

$$R = \prod_{i=1}^{m-1} F^{(i)}(x) = \beta_1 + \beta_2 x + \cdots,$$

where $\beta_1, \beta_2, \ldots$ are integers of the field k. Then $FR = nU$ where n is a rational integer and U is a polynomial whose (integer) coefficients have no common factor. From this it follows that n is congruent to 0 modulo the product of the two ideals $\mathfrak{a}$ and $\mathfrak{b} = (\beta_1, \beta_2, \ldots)$. Lemma 2 shows moreover that conversely each number $\alpha_i\beta_h$ is divisible by n. Hence we have $\mathfrak{ab} = n$.

Theorem 9. *Let $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ be ideals such that $\mathfrak{ac} = \mathfrak{bc}$; if $\mathfrak{c} \neq 0$ then $\mathfrak{a} = \mathfrak{b}$.*

Proof. Let $\mathfrak{m}$ be an ideal such that $\mathfrak{cm}$ is a principal ideal (α). Since $\mathfrak{ac} = \mathfrak{bc}$ we have $\mathfrak{acm} = \mathfrak{bcm}$ or $\alpha\mathfrak{a} = \alpha\mathfrak{b}$, whence $\mathfrak{a} = \mathfrak{b}$.

Theorem 10. *If all the numbers of an ideal* $\mathfrak{c}$ *are congruent to* 0 *modulo an ideal* $\mathfrak{a}$ *then* $\mathfrak{c}$ *is divisible by* $\mathfrak{a}$.

Proof. Let $\mathfrak{m}$ be an ideal such that $\mathfrak{am}$ is a principal ideal (α). Then all the numbers of the ideal $\mathfrak{mc}$ are divisible by α and consequently there is an ideal $\mathfrak{b}$ such that $\mathfrak{mc} = \alpha\mathfrak{b}$. Then $\mathfrak{amc} = \alpha\mathfrak{ab}$, i.e. $\alpha\mathfrak{c} = \alpha\mathfrak{ab}$ and so $\mathfrak{c} = \mathfrak{ab}$.

Theorem 11. *If the product* $\mathfrak{ab}$ *of two ideals is divisible by a prime ideal* $\mathfrak{p}$ *then at least one of the ideals* $\mathfrak{a}$, $\mathfrak{b}$ *is divisible by* $\mathfrak{p}$.

Proof. Suppose $\mathfrak{a}$ is not divisible by $\mathfrak{p}$. Then the ideal $(\mathfrak{a}, \mathfrak{p})$ is a divisor of $\mathfrak{p}$ distinct from $\mathfrak{p}$ and hence must be (1). Thus 1 can be expressed as $1 = \alpha + \pi$ where α is a number in $\mathfrak{a}$ and π is a number in $\mathfrak{p}$. Hence if β is any number in $\mathfrak{b}$ we have $\beta = \alpha\beta + \pi\beta \equiv \alpha\beta \pmod{\mathfrak{p}}$. By hypothesis $\alpha\beta \equiv 0 \pmod{\mathfrak{p}}$ and consequently $\beta \equiv 0 \pmod{\mathfrak{p}}$. Thus $\mathfrak{b}$ is divisible by $\mathfrak{p}$.

We can now prove Theorem 7, the fundamental theorem of ideal theory, as follows: if $\mathfrak{i}$ is not itself a prime ideal let $\mathfrak{i} = \mathfrak{ab}$ where $\mathfrak{a}$ is a divisor of $\mathfrak{i}$ distinct from $\mathfrak{i}$ and 1. If now one of the factors $\mathfrak{a}$, $\mathfrak{b}$ is not a prime ideal we can represent it in the same way as a product, obtaining a factorisation $\mathfrak{i} = \mathfrak{a}'\mathfrak{b}'\mathfrak{c}'$, and proceed in this way. The procedure terminates because, according to Lemma 1, there are only finitely many divisors of the ideal $\mathfrak{i}$. If r is this finite number of divisors then $\mathfrak{i}$ cannot be expressed as a product of more than r factors, for a representation of the form $\mathfrak{i} = \mathfrak{a}_1 \ldots \mathfrak{a}_{r+1}$ would imply the existence of $r + 1$ mutually distinct ideal factors

$$\mathfrak{a}_1, \mathfrak{a}_1\mathfrak{a}_2, \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3, \ldots, \mathfrak{a}_1 \cdots \mathfrak{a}_{r+1}.$$

The final stage of the procedure produces the desired representation

$$\mathfrak{i} = \mathfrak{pq} \cdots \mathfrak{l}.$$

This representation is unique. For if we also had $\mathfrak{i} = \mathfrak{p}'\mathfrak{q}' \cdots \mathfrak{l}'$ then $\mathfrak{i}$ would be divisible by $\mathfrak{p}'$ and hence, by Theorem 11, one of the factors $\mathfrak{p}$, $\mathfrak{q}$, …, $\mathfrak{l}$, say $\mathfrak{p}$, would be divisible by $\mathfrak{p}'$; hence we would have $\mathfrak{p} = \mathfrak{p}'$ and consequently, by Theorem 9, the equation $\mathfrak{q} \cdots \mathfrak{l} = \mathfrak{q}' \cdots \mathfrak{l}'$ and we deal with this in the same way.

The fundamental Theorem 7 has the following easy consequence.

Theorem 12. *Every ideal* $\mathfrak{i}$ *of the field* k *can be expressed as the greatest common divisor of two integers* κ, ρ.

Proof. Let κ be any integer divisible by $\mathfrak{i}$. If there were an integer ρ divisible by $\mathfrak{i}$ such that $\rho/\mathfrak{i}$ is prime to $\kappa/\mathfrak{i}$ then we would have $\mathfrak{i} = (\kappa, \rho)$.

We find such an integer ρ as follows: let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be all the prime ideals dividing κ; if $\mathfrak{i} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$ where the $a_i \geq 0$ then the r ideals $\mathfrak{d}_i = \mathfrak{p}_1^{a_1+1} \cdots \mathfrak{p}_{i-1}^{a_{i-1}+1} \mathfrak{p}_{i+1}^{a_{i+1}+1} \cdots \mathfrak{p}_r^{a_r+1}$ have no common factor. So there are r numbers δ_i, with δ_i in $\mathfrak{d}_i$, such that

$$\delta_1 + \delta_2 + \cdots + \delta_r = 1.$$

If α_i is any number which belongs to $\mathfrak{p}_i^{a_i}$ but not to $\mathfrak{p}_i^{a_i+1}$ and we define

$$\rho = \alpha_1 \delta_1 + \cdots + \alpha_r \delta_r$$

then ρ is precisely divisible by each $\mathfrak{p}_i^{a_i}$ but not by $\mathfrak{p}_i^{a_i+1}$.

§6. Forms of Number Fields and Their Contents

The Kronecker theory of forms (*Kronecker* (16)) is concerned with the following additional concepts.

A polynomial F in arbitrary many variables u, v, ..., whose coefficients are algebraic integers of a field k is called a *form* of k. The *conjugate forms* F', ..., $F^{(m-1)}$ of a form F are obtained by replacing the coefficients of F in order by their respective conjugates. The product of F with all its conjugates is a polynomial in the variables u, v, ... with rational integral coefficients; we may write this polynomial in the form $nU(u, v, \ldots)$ where n is a positive rational integer and U is a polynomial whose coefficients are rational integers with no common factor. We call n the *norm of the form F*. When the norm of F is 1 we call F a *unit form*. A polynomial whose coefficients are rational integers with no common factor is called a *rational unit form*. Two forms are said to be *content-equal*[1] to one another (denoted by $\simeq$) when their quotient is equal to the quotient of two unit forms. In particular, every unit form $\simeq 1$. A form H is said to be *divisible* by the form F if there exists a form G such that $H \simeq FG$. A form P is called a *prime form* when P is not divisible (in the sense of content-equality) by any form other than 1 and itself.

The relation of Kronecker's theory of forms to ideal theory becomes clear when we remark that to every ideal $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$ a form F can be constructed by multiplying the numbers α_1, ..., α_r by arbitrary distinct products of powers of the indeterminates u, v, ... and adding the resulting products. Conversely, each form F with coefficients α_1, ..., α_r produces an ideal $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$. This ideal $\mathfrak{a}$ is called the *content* of the form F. We have now the following.

[1] In Kronecker's terminology "equivalent in the narrow sense"

Theorem 13. *The content of the product of two forms is equal to the product of their contents.*

Proof. Let F and G be forms with arbitrary variables and coefficients $\alpha_1, \ldots, \alpha_r$ and $\beta_1, \ldots, \beta_s$ respectively and let the coefficients of the product $H = FG$ be $\gamma_1, \ldots, \gamma_t$. Further, let $\mathfrak{p}^a$ and $\mathfrak{p}^b$ be the highest powers of a prime ideal $\mathfrak{p}$ which divide $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$ and $\mathfrak{b} = (\beta_1, \ldots, \beta_s)$ respectively. Let us arrange the terms of the two forms F and G first of all according to decreasing powers of u and then, for each power of u, according to decreasing powers of v and so on. Let $\alpha u^h v^l \cdots$ be the first term of F in this arrangement whose coefficient α is divisible by no higher power of $\mathfrak{p}$ than the a-th; and let $\beta u^{h'} v^{l'}$ be the first term of G whose coefficient β is divisible by no higher power of $\mathfrak{p}$ than the b-th. Then obviously the coefficient γ of $\gamma u^{h+h'} v^{l+l'} \ldots$ in H is divisible by no higher power of $\mathfrak{p}$ than the $(a+b)$-th. All the remaining coefficients of H are, however, also divisible by $\mathfrak{p}^{a+b}$. The assertion that $(\alpha_1, \ldots, \alpha_r)(\beta_1, \ldots, \beta_s) = (\gamma_1, \ldots, \gamma_t)$ follows at once.

We have, in particular, as an easy consequence of Theorem 13, that each unit form has content 1 and, conversely, that each form whose coefficients have greatest common ideal divisor 1 is a unit form. It follows that content-equal forms have the same content and, conversely, that all forms with the same content are content-equal. In particular any two forms with the same coefficients are content-equal.

Further consequences of Theorem 13 are as follows.

Theorem 14. *For any given form F there exists a form R such that FR is content-equal to an integer.*

Theorem 15. *If the product of two forms is divisible by a prime form P then at least one of the two forms is divisible by P.*

Theorem 16. *Every form can be represented (in the sense of content-equality) in one and only one way as a product of prime forms.*

These theorems run parallel to Theorems 8 and 11 and the fundamental Theorem 7 of ideal theory.

Apart from the ways followed by Dedekind and Kronecker there are in addition two simpler approaches to the proof of the fundamental Theorem

7. One method is based on the theory of Galois number fields; see Sect. 36 (*Hilbert* (2,3)). The second method proceeds from the theorem that the ideals of a field are distributed into a finite number of ideal classes. The basic idea of the proof can be viewed as a generalisation of that which leads to the well-known Euclidean algorithm to determine the greatest common divisor of two rational integers (*Hurwitz* (3)).

3. Congruences with Respect to Ideals

§7. The Norm of an Ideal and its Properties

The theory of the factorisation of ideals in a field which we developed in Chapter 2 allows us to carry over to the numbers of an algebraic number field the elementary theorems of the theory of rational numbers. We describe first the following general ideas and results.

The maximum number of algebraic integers of a field which are incongruent to one another modulo an ideal $\mathfrak{a}$ is called the *norm of the ideal* $\mathfrak{a}$ and is denoted by $n(\mathfrak{a})$.

Theorem 17. *The norm of a prime ideal* $\mathfrak{p}$ *is a power of the rational prime* p *divisible by* $\mathfrak{p}$.

Proof. Suppose there are f integers $\omega_1, \ldots, \omega_f$ of a basis for the field which are independent in the sense that they satisfy no congruence of the form

$$a_1\omega_1 + \cdots + a_f\omega_f \equiv 0 \qquad (\text{mod } \mathfrak{p})$$

with $a_1, \ldots, a_f$ rational integers not all divisible by p and which have the further property that each of the remaining $m - f$ integers of the basis is congruent modulo $\mathfrak{p}$ to an expression of the form $a_1\omega_1 + \cdots + a_f\omega_f$. Then every integer of the field is congruent modulo $\mathfrak{p}$ to such an expression and it follows at once that there are exactly p^f mutually incongruent integers modulo $\mathfrak{p}$.

The exponent f is called the *degree of the prime ideal* $\mathfrak{p}$.

Theorem 18. *The norm of the product* $\mathfrak{ab}$ *of two ideals is equal to the product of their norms.*

Proof. Let α be a number divisible by $\mathfrak{a}$ chosen as in the proof of Theorem 12 so that $\alpha/\mathfrak{a}$ is an ideal prime to $\mathfrak{b}$. If ξ runs through a set of $n(\mathfrak{a})$ integers incongruent to one another modulo $\mathfrak{a}$ and η through a set of $n(\mathfrak{b})$ integers incongruent to one another modulo $\mathfrak{b}$ the expression $\xi + \alpha\eta$ produces a com-

plete set of integers incongruent to one another modulo $\mathfrak{ab}$; this set consists of $n(\mathfrak{a})n(\mathfrak{b})$ integers.

Theorem 19. *Let*

$$\begin{aligned}\iota_1 &= a_{11}\omega_1 + \cdots + a_{1m}\omega_m,\\ &\ldots\ldots,\\ \iota_m &= a_{m1}\omega_1 + \cdots + a_{mm}\omega_m\end{aligned}$$

be a basis for an ideal $\mathfrak{a}$. Then its norm $n(\mathfrak{a})$ is equal to the absolute value of the determinant of the coefficients a.

Proof. Let us consider the original basis for $\mathfrak{a}$ which we found in the proof of Theorem 6. In this basis the coefficients a_{rs} are all zero for $s > r$ and the coefficients a_{rr} are all positive. Thus the determinant of the coefficients a is the product $a_{11} \ldots a_{mm}$. On the other hand the expression

$$u_1\omega_1 + \cdots + u_m\omega_m$$

for

$$u_1 = 0, 1, \ldots, a_{11} - 1, \ldots, u_m = 0, 1, \ldots, a_{mm} - 1$$

represents a complete set of integers mutually incongruent modulo $\mathfrak{a}$. This completes the proof of Theorem 19. The converse of the theorem is obvious.

The connexion with Kronecker's theory of forms becomes clear from the following theorem.

Theorem 20. *Let F be a form with content $\mathfrak{a}$. Then the norm of the form F is equal to the norm of the ideal $\mathfrak{a}$, i.e. $n(F) = n(\mathfrak{a})$. In particular the absolute value of the norm of an integer α is equal to the norm of the principal ideal (α).*

Proof. Let $\iota_1, \ldots, \iota_m$ be a basis for the ideal $\mathfrak{a}$ and consider the form

$$F = \iota_1 u_1 + \cdots + \iota_m u_m.$$

Then we have

$$\begin{aligned}\omega_1 F &= l_{11}\iota_1 + \cdots + l_{1m}\iota_m,\\ &\ldots\ldots\\ \omega_m F &= l_{m1}\iota_1 + \cdots + l_{mm}\iota_m,\end{aligned}$$

where $l_{11}, \ldots, l_{mm}$ are linear forms in $u_1, \ldots, u_m$ with rational integral coefficients. We prove first that the determinant $|l_{rs}|$ of the

forms $l_{11}, \ldots, l_{mm}$ is a rational unit form. Suppose to the contrary that the coefficients of the determinant $|l_{rs}|$ were all divisible by a prime number p. Then there would be m forms $L_1, \ldots, L_m$ with rational integer coefficients not all divisible by p such that

$$\begin{aligned} L_1 l_{11} + \cdots + L_m l_{m1} &\equiv 0 \qquad (\text{mod } p), \\ &\cdots\cdots \\ L_1 l_{1m} + \cdots + L_m l_{mm} &\equiv 0 \qquad (\text{mod } p). \end{aligned}$$

From this it follows that

$$(L_1\omega_1 + \cdots + L_m\omega_m)F \equiv 0 \qquad (\text{mod } p\mathfrak{a}).$$

So the product $\mathfrak{l}\mathfrak{a}$ is divisible by $p\mathfrak{a}$, where $\mathfrak{l}$ is the content of the form $L_1\omega_1 + \cdots + L_m\omega_m$. Hence $\mathfrak{l}$ is divisible by p: but this cannot happen since a number of the form $a_1\omega_1 + \cdots + a_m\omega_m$ with rational integer coefficients $a_1, \ldots, a_m$ can be divisible by p only if all the coefficients $a_1, \ldots, a_m$ are divisible by p.

By the multiplication theorem for determinants we have

$$\begin{vmatrix} \omega_1 F & \cdots & \omega_m F \\ \omega_1' F' & \cdots & \omega_m' F' \\ & \cdots & \\ \omega_1^{(m-1)} F^{(m-1)} & \cdots & \omega_m^{(m-1)} F^{(m-1)} \end{vmatrix} = \begin{vmatrix} l_{11} & \cdots & l_{1m} \\ l_{21} & \cdots & l_{2m} \\ & \cdots & \\ l_{m1} & \cdots & l_{mm} \end{vmatrix} \begin{vmatrix} \iota_1 & \cdots & \iota_m \\ \iota_1' & \cdots & \iota_m' \\ & \cdots & \\ \iota_1^{(m-1)} & \cdots & \iota_m^{(m-1)} \end{vmatrix}$$

and hence by cancellation of the factor

$$\begin{vmatrix} \omega_1 & \cdots & \omega_m \\ \omega_1' & \cdots & \omega_m' \\ & \cdots & \\ \omega_1^{(m-1)} & \cdots & \omega_m^{(m-1)} \end{vmatrix}$$

we have the relation $FF' \ldots F^{(m-1)} \simeq n(\mathfrak{a})$, or $n(F) = n(\mathfrak{a})$. The second part of the theorem follows when we set $F = \alpha(u_1\omega_1 + \cdots + u_m\omega_m)$.

When we apply the substitution $t' = (\vartheta : \vartheta')$ to all the numbers $\alpha_1, \alpha_2, \ldots$ of an ideal $\mathfrak{a}$ the resulting ideal $\mathfrak{a}' = (t'\alpha_1, t'\alpha_2, \ldots)$ is called the *ideal conjugate to* $\mathfrak{a}$ by the substitution t'. If we consider the composite field of $k, k', \ldots, k^{(m-1)}$ Theorems 18 and 20 show us that the product of $\mathfrak{a}$ and all

its conjugate ideals is a rational integer, namely $n(\mathfrak{a})$.[1] From this fact arises a new definition of the norm of the ideal $\mathfrak{a}$ which corresponds precisely to the definition of the norm of a number α and which moreover is capable of an important generalisation. See Sect. 14.

Theorem 21. *In each ideal $\mathfrak{i}$ there can be found two numbers such that the greatest common divisor of their norms is the norm of $\mathfrak{i}$.*

Proof. Let $a = n(\mathfrak{i})$. As in the proof of Theorem 12 we find a number α in $\mathfrak{i}$ such that $\alpha/\mathfrak{i}$ is prime to a. Then, if $\alpha', \ldots, \alpha^{(m-1)}$ are the numbers conjugate to α and $\mathfrak{i}', \ldots, \mathfrak{i}^{(m-1)}$ are the ideals conjugate to $\mathfrak{i}$, we have $\alpha'/\mathfrak{i}', \ldots, \alpha^{(m-1)}/\mathfrak{i}^{(m-1)}$ and hence $n(\alpha)/n(\mathfrak{i}) = n(\alpha)/a$ prime to a. Hence $n(\mathfrak{i}) = a = (a^m, n(\alpha)) = (n(a), n(\alpha))$.

§8. Fermat's Theorem in Ideal Theory. The Function $\varphi(\mathfrak{a})$

As a result of the same considerations as in the theory of rational numbers we have the following result corresponding to the Fermat theorem (*Dedekind* (1)).

Theorem 22. *If $\mathfrak{p}$ is a prime ideal of degree f then every integer ω of the field k satisfies the congruence*

$$\omega^{p^f} \equiv \omega \qquad (\text{mod } \mathfrak{p}).$$

The generalised Fermat theorem is also easily carried over to the number field situation. The following theorems can also be proved without difficulty (*Dedekind* (1)).

Theorem 23. *The number of integers incongruent to one another modulo an ideal $\mathfrak{a}$ and prime to $\mathfrak{a}$ is*

$$\varphi(\mathfrak{a}) = n(\mathfrak{a})\left(1 - \frac{1}{n(\mathfrak{p}_1)}\right)\left(1 - \frac{1}{n(\mathfrak{p}_2)}\right)\cdots\left(1 - \frac{1}{n(\mathfrak{p}_r)}\right)$$

where $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ are all the distinct prime ideals dividing $\mathfrak{a}$.

If the ideals $\mathfrak{a}$ and $\mathfrak{b}$ are prime to one another we have

$$\varphi(\mathfrak{a}\mathfrak{b}) = \varphi(\mathfrak{a})\varphi(\mathfrak{b})$$

[1] See p.34 paragraph 2.

and for each ideal $\mathfrak{a}$ *we have*

$$\sum \varphi(\mathfrak{t}) = n(\mathfrak{a})$$

where the summation extends over all the ideals $\mathfrak{t}$ *dividing* $\mathfrak{a}$.

Theorem 24. *Every integer* ω *prime to an ideal* $\mathfrak{a}$ *satisfies the congruence*

$$\omega^{\varphi(\mathfrak{a})} \equiv 1 \pmod{\mathfrak{a}}.$$

For example, if $\mathfrak{p}$ *is a prime ideal of degree* f *then every integer* ω *prime to* $\mathfrak{p}$ *satisfies the congruence*

$$\omega^{p^f(p^f-1)} \equiv 1 \pmod{\mathfrak{p}^2}.$$

We have also the following results.

Theorem 25. *If* $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ *are ideals pairwise prime to one another and* $\alpha_1, \ldots, \alpha_r$ *are arbitrary integers then there exists an integer* ω *which satisfies the congruences*

$$\omega \equiv \alpha_1 \pmod{\mathfrak{a}_1}, \ldots, \omega \equiv \alpha_r \pmod{\mathfrak{a}_r}.$$

Theorem 26. *A congruence of degree* r *modulo a prime ideal* $\mathfrak{p}$ *of the form*

$$\alpha x^r + \alpha_1 x^{r-1} + \cdots + \alpha_r \equiv 0 \pmod{\mathfrak{p}}$$

where $\alpha, \alpha_1, \ldots, \alpha_r$ *are integers in* k *and* $\alpha \not\equiv 0$ *(mod* $\mathfrak{p}$*) has at most* r *roots incongruent to one another modulo* $\mathfrak{p}$.

Theorem 27. *Let* $\mathfrak{p}$ *be a prime ideal which divides the rational prime number* p. *If* α *is a root of the congruence*

$$a x^r + a_1 x^{r-1} + \cdots + a_r \equiv 0 \pmod{\mathfrak{p}}$$

where $a, a_1, \ldots, a_r$ *are rational integers, then* α^p *is also a root of the same congruence.*

Proof. We denote the left hand side of the congruence by $F(x)$. Then, according to the Fermat theorem, we see that the congruence $F(x^p) \equiv (F(x))^p$ (mod p) holds identically in x, and this fact implies the assertion of the theorem.

§9. Primitive Roots for a Prime Ideal

An integer ρ of the field k is called a *primitive root for* a prime ideal $\mathfrak{p}$ when the first $p^f - 1$ powers of ρ form a complete set of $p^f - 1$ integers prime to $\mathfrak{p}$ which are mutually incongruent modulo $\mathfrak{p}$. Here again the same reasoning as in the rational number case leads easily to the following result.

Theorem 28. *There are $\Phi(p^f - 1)$ primitive roots for the prime ideal $\mathfrak{p}$, where $\Phi(p^f - 1)$ is the number of rational integers incongruent to one another modulo $p^f - 1$ and prime to $p^f - 1$.*

A theory of primitive roots for the powers of a prime ideal $\mathfrak{p}$ has not yet been developed; but we can easily obtain the following (*Dedekind* (6)).

Theorem 29. *Let $\mathfrak{p}$ be a prime ideal of the field k. Then there exists an integer ρ of k such that every other integer of k is congruent modulo an arbitrarily high power $\mathfrak{p}^l$ of $\mathfrak{p}$ to a certain polynomial in ρ with rational integer coefficients.*

Proof. Let ρ^* be any primitive root for $\mathfrak{p}$. Then obviously each integer in k is congruent modulo $\mathfrak{p}$ to a certain polynomial in ρ^*. Let

$$P(\rho^*) \equiv 0 \qquad (\text{mod } \mathfrak{p})$$

be the congruence modulo $\mathfrak{p}$ of lowest degree with rational integer coefficients satisfied by ρ^*. If the degree of P is f' no expression of the form

$$a_1 + a_2\rho^* + \cdots + a_{f'}(\rho^*)^{f'-1}$$

with rational integer coefficients $a_1, a_2, \ldots, a_{f'}$ can be congruent to 0 modulo $\mathfrak{p}$ unless all the coefficients $a_1, a_2, \ldots, a_{f'}$ are congruent to 0 modulo p. Since on the other hand every integer of the field must be congruent to an expression of the above form it follows that $f = f'$.

In the situation where $P(\rho^*) \equiv 0$ modulo $\mathfrak{p}^2$ we set $\rho = \rho^* + \pi$ where π is an integer divisible by $\mathfrak{p}$ but not by $\mathfrak{p}^2$. Then since, according to Theorem 27,

$$\frac{dP(\rho^*)}{d\rho^*} = (\rho^* - (\rho^*)^p) \cdots (\rho^* - (\rho^*)^{p^{f-1}}) \not\equiv 0 \qquad (\text{mod } \mathfrak{p}),$$

we must have

$$P(\rho) = P(\rho^* + \pi) \equiv P(\rho^*) + \pi \frac{dP(\rho^*)}{d\rho^*} \not\equiv 0 \qquad (\text{mod } \mathfrak{p}^2).$$

The number ρ has the desired property. If $\alpha_1, \alpha_2, \ldots, \alpha_l$ run through all expressions of the form $a_1 + a_2\rho + \ldots + a_f\rho^{f-1}$ where $a_1, a_2, \ldots, a_f$ are integers from the range $0, 1, \ldots, p-1$, it is easily seen that the sums

$$\alpha_1 + \alpha_2 P(\rho) + \cdots + \alpha_l\{P(\rho)\}^{l-1}$$

represent integers incongruent to one another modulo $\mathfrak{p}^l$; and since there are p^{fl} numbers of this form it follows that they exhaust all the incongruent residues modulo $\mathfrak{p}^l$. Clearly the same property holds for all integers congruent to ρ modulo $\mathfrak{p}^2$.

We use this last result to give the following representation of the ideal $\mathfrak{p}$.

Theorem 30. *Let $\mathfrak{p}$ be a prime ideal of degree f. Then there is an integer ρ in k with the property described in Theorem 29 such that*

$$\mathfrak{p} = (p, P(\rho))$$

where $P(\rho)$ is a polynomial in ρ of degree f with rational integer coefficients.

Proof. Let $p = \mathfrak{p}^e\mathfrak{a}$ where $\mathfrak{a}$ is an ideal not divisible by $\mathfrak{p}$. Let α be an integer not divisible by $\mathfrak{p}$, though possibly by $\mathfrak{a}$. According to Theorem 24 we have $\alpha^{p^f(p^f-1)} \equiv 1 \pmod{\mathfrak{p}^2}$. If we replace the number ρ found in the previous proof by $\rho\alpha^{p^f(p^f-1)}$ the new number ρ still has the property of Theorem 29. Since the last coefficient of the polynomial $P(\rho)$ cannot be divisible by p it follows that for the new number ρ we must have $P(\rho)$ prime to $\mathfrak{a}$, i.e. $\mathfrak{p} = (p, P(\rho))$.

4. The Discriminant of a Field and its Divisors

§10. Theorem on the Divisors of the Discriminant. Lemma on Integral Functions

The *discriminant* d of a field k is defined by the equation

$$d = \begin{vmatrix} \omega_1 & \cdots & \omega_m \\ \omega_1' & \cdots & \omega_m' \\ & \cdots\cdots & \\ \omega_1^{(m-1)} & \cdots & \omega_m^{(m-1)} \end{vmatrix}^2$$

where $\omega_1, \ldots, \omega_m$ form a basis for k; the discriminant d is a rational integer. For the development of field theory the investigation of the ideal factors of the discriminant is of central importance. We have the following fundamental theorem.

Theorem 31. *The rational prime numbers which divide the discriminant d of a number field k are precisely those primes which are divisible by the square of a prime ideal of k.*

The proof of this theorem has given rise to considerable difficulty; it was first carried through by Dedekind (*Dedekind* (6)). Hensel has given a second proof and thereby supplemented the Kronecker theory of algebraic numbers in an important respect. Hensel's proof depends on the following ideas introduced by Kronecker (*Kronecker* (16), *Hensel* (4)).

Let $u_1, \ldots, u_m$ be indeterminates, and let $\omega_1, \ldots, \omega_m$ be a basis; then

$$\xi = \omega_1 u_1 + \cdots + \omega_m u_m$$

is called the *fundamental form* of the field k. This obviously satisfies the equation

$$(x - \omega_1 u_1 - \cdots - \omega_m u_m)(x - \omega_1' u_1 - \cdots - \omega_m' u_m) \cdots$$
$$\cdots (x - \omega_1^{(m-1)} u_1 - \cdots - \omega_m^{(m-1)} u_m) = 0$$

which can be put in the form

$$x^m + U_1 x^{m-1} + U_2 x^{m-2} + \cdots + U_m = 0$$

where $U_1, \ldots, U_m$ are polynomials in $u_1, \ldots, u_m$ with rational integer coefficients. This equation of degree m is called the *fundamental equation*. In order to be able to work with the concepts just described it is necessary to carry over the theorems concerning factorisation of polynomials in one variable x modulo a rational prime number p (*Serret* (1)) to the more general case where the polynomials contain not only the variable x but also the m indeterminates $u_1, \ldots, u_m$ as parameters.

In what follows we shall always use the term *integer polynomial* to mean a polynomial in variables or indeterminates with *rational integer* coefficients. An integer polynomial $Z(x; u_1, \ldots, u_m)$ is said to be *divisible modulo p* by another integer polynomial $X(x; u_1, \ldots, u_m)$ if there exists a third integer polynomial $Y(x; u_1, \ldots, u_m)$ such that the congruence

$$Z \equiv XY \pmod{p}$$

holds identically in the variables $x, u_1, \ldots, u_m$. An integer polynomial P is called a *prime polynomial modulo p* if it is divisible modulo p by no integer polynomials other than those which are congruent modulo p to a rational integer or to P itself or to a product of P by a rational integer. The usual laws of divisibility of polynomials of *one* variable hold here also; in particular we have the following result which is easily established using the well-known Euclidean recursive procedure.

Theorem 32. *If X and Y are integer polynomials in $x, u_1, \ldots, u_m$ which have no common divisor modulo the rational prime number p then there exists an integer polynomial U in $u_1, \ldots, u_m$ alone which is not congruent to* 0 *modulo p such that*

$$U \equiv AX + BY \pmod{p}$$

where A and B are suitable integer polynomials in $x, u_1, \ldots, u_m$.

Our next object is the factorisation of the left hand side F of the fundamental equation into prime polynomials modulo the prime p. We first prove the following lemma.

Lemma 3. *If $\mathfrak{p}$ is a prime ideal of degree f dividing p then there exists a prime polynomial modulo p, $\Pi(x; u_1, \ldots, u_m)$, of degree f in x such that when x is replaced by the fundamental form ξ the coefficients of the powers and products of $u_1, \ldots, u_m$ in $\Pi(\xi; u_1, \ldots, u_m)$ are divisible by $\mathfrak{p}$ but are not all divisible by $\mathfrak{p}^2$ nor by any prime ideal distinct from $\mathfrak{p}$ which divides p.*

Proof. Let $p = \mathfrak{p}^e \mathfrak{a}$ where the ideal $\mathfrak{a}$ is not divisible by $\mathfrak{p}$. Let ρ be a primitive root for $\mathfrak{p}$ which has the properties described in Theorems 29 and 30. Let $P(\rho)$ be an integer polynomial of degree f associated with $\mathfrak{p}$ (as in

Theorems 29 and 30) such that $\mathfrak{p} = (p, P(\rho))$. $P(x)$ is a prime polynomial modulo p, for otherwise ρ would satisfy a congruence modulo $\mathfrak{p}$ of degree less than f. We set

$$\rho = a_1\omega_1 + \cdots + a_m\omega_m,$$

where $a_1, \ldots, a_m$ are rational integers, and suppose that the coefficient of ρ^f in $P(\rho)$ is 1. Since $P(\rho) \equiv 0 \pmod{\mathfrak{p}}$ it follows from Theorem 27 that we have also $P(\rho^p) \equiv 0$, $P(\rho^{p^2}) \equiv 0, \ldots, P(\rho^{p^{f-1}}) \equiv 0 \pmod{\mathfrak{p}}$; so the congruence $P(x) \equiv 0 \pmod{\mathfrak{p}}$ has the f mutually incongruent roots $\rho, \rho^p, \ldots, \rho^{p^{f-1}}$ and hence

$$P(x) \equiv (x-\rho)(x-\rho^p)\cdots(x-\rho^{p^{f-1}}) \pmod{\mathfrak{p}}$$

identically in x. Thus the elementary symmetric functions of $\rho, \rho^p, \ldots, \rho^{p^{f-1}}$ are all congruent modulo $\mathfrak{p}$ to certain rational integers.

Since each integer of the field k is congruent modulo $\mathfrak{p}$ to a polynomial in ρ we can write

$$\xi \equiv L(\rho; u_1, \ldots, u_m) \pmod{\mathfrak{p}}$$

where L is an integer polynomial in ρ, $u_1, \ldots, u_m$. According to what was proved above the expression

$$(x - L(\rho; u_1, \ldots, u_m))(x - L(\rho^p; u_1, \ldots, u_m))\cdots(x - L(\rho^{p^{f-1}}; u_1, \ldots, u_m))$$

is congruent modulo $\mathfrak{p}$ to an integer polynomial in x, $u_1, \ldots, u_m$; we write this polynomial in the form

$$\Pi(x; u_1, \ldots, u_m) = x^f + V_1x^{f-1} + \cdots + V_f,$$

where $V_1, \ldots, V_f$ are integer polynomials in $u_1, \ldots, u_m$. Obviously the fundamental form ξ satisfies the congruence in x

$$\Pi(x; u_1, \ldots, u_m) \equiv 0 \pmod{\mathfrak{p}}.$$

Since the polynomial $\Pi(x; a_1, \ldots, a_m) \equiv P(x)$ modulo $\mathfrak{p}$ it follows that $\mathfrak{p} = (p, \Pi(\rho; a_1, \ldots, a_m))$ and hence the coefficients of the powers and products of $u_1, \ldots, u_m$ in $\Pi(x; u_1, \ldots, u_m)$ are not all divisible by $\mathfrak{p}^2$ nor by any prime ideal distinct from $\mathfrak{p}$ dividing $\mathfrak{a}$. Since $P(x)$ is a prime polynomial, so also *a fortiori* is $\Pi(x; u_1, \ldots, u_m)$.

Lemma 4. *If $\Phi(x; u_1, \ldots, u_m)$ is an integer polynomial which is congruent to 0 modulo p identically in $u_1, \ldots, u_m$ as soon as we replace x by the fundamental form ξ then $\Phi(x; u_1, \ldots, u_m)$ is divisible modulo p by $\Pi(x; u_1, \ldots, u_m)$.*

Proof. Suppose, to the contrary, that Φ and Π have no common factor modulo p. Then, according to Theorem 32, there is an integer polynomial U in $u_1, \ldots, u_m$ alone, not congruent to 0 modulo p, such that $U \equiv A\Phi + B\Pi$ modulo p, where A and B are integer polynomials in x, $u_1, \ldots, u_m$. From

this it follows, when we replace x by the fundamental form ξ, that $U \equiv 0$ modulo $\mathfrak{p}$ and hence modulo p, which is not the case.

Lemma 5. *Let Φ be an integer polynomial in x, $u_1, \ldots, u_m$ which is congruent to 0 modulo $\mathfrak{p}^e$ identically in $u_1, \ldots, u_m$ whenever x is replaced by the fundamental form ξ. Then Φ is divisible modulo p by Π^e.*

Proof. Suppose $\Phi \equiv \Pi^{e'} F \pmod p$ where $e' < e$ and F is an integer polynomial in x, $u_1, \ldots, u_m$ which is not divisible modulo p by Π. Then it follows that all the coefficients of powers and products of $u_1, \ldots, u_m$ in $\{\Pi(\xi; u_1, \ldots, u_m)\}^{e'} F(\xi; u_1, \ldots, u_m)$ must be divisible by $\mathfrak{p}^e$. Let $\Pi(\xi; u_1, \ldots, u_m)$ and $F(\xi; u_1, \ldots, u_m)$ be arranged according to descending powers of u_1, the coefficients of powers of u_1 according to descending powers of u_2 and so on. If then π is the first coefficient in $\Pi(\xi)$ which is not divisible by $\mathfrak{p}^2$ and κ the first coefficient in $F(\xi)$ which is not divisible by $\mathfrak{p}$ (if there are any such) then we would have $\pi^{e'}\kappa \equiv 0 \pmod{\mathfrak{p}^e}$ which is not possible. So all the coefficients of $F(\xi)$ are divisible by $\mathfrak{p}$; hence it follows by Lemma 4 that $F(x; u_1, \ldots, u_m)$ is divisible modulo p by $\Pi(\xi; u_1, \ldots, u_m)$. This contradicts our hypothesis.

§11. Factorisation and Discriminant of the Fundamental Equation

From Lemmas 3, 4 and 5 we deduce the following important facts concerning the factorisation of the left hand side of the fundamental equation.

Theorem 33. *If the rational prime number p factorises as $p = \mathfrak{p}^e(\mathfrak{p}')^{e'} \ldots$ then the left hand side F of the fundamental equation decomposes modulo p in the form*

$$F \equiv \Pi^e (\Pi')^{e'} \cdots \pmod p,$$

where Π, Π', ... are distinct prime polynomials modulo p; further, if

$$F = \Pi^e (\Pi')^{e'} \cdots + pG$$

then G is an integer polynomial in the variables x, $u_1, \ldots, u_m$ which is not divisible modulo p by any of the prime polynomials Π, Π', ...

Theorem 34. *The congruence of degree m*

$$F(x; u_1, \ldots, u_m) \equiv 0 \pmod p$$

derived from the fundamental equation is the congruence of lowest degree in x with rational integral coefficients which is satisfied modulo p by the fundamental form ξ.

Proof. Let Φ be an integer polynomial in $x, u_1, \dots, u_m$ such that the congruence $\Phi(x) \equiv 0 \pmod p$ is satisfied by the fundamental form ξ. Let the distinct prime ideal divisors $\mathfrak{p}, \mathfrak{p}', \dots$ of p have degrees $f, f', \dots$ respectively. Taking norms we have $p^m = p^{fe+f'e'+\cdots}$, and so $m = fe+f'e'+\cdots$. Let Π, Π', ... be the prime polynomials in $x, u_1, \dots, u_m$ belonging to the prime ideals $\mathfrak{p}, \mathfrak{p}', \dots$ respectively as in the preceding lemmas. It follows from Lemma 5 that

$$\Phi \equiv \Pi^e (\Pi')^{e'} \cdots \Psi \pmod p,$$

where Ψ is an integer polynomial. Since $\Pi, \Pi', \dots$ have degrees $f, f', \dots$ respectively, it follows that Φ must be of degree at least m in x. When we take Φ to be the left hand side F of the fundamental equation we obtain the assertions of Theorem 34 and the first part of Theorem 33.

Finally, suppose $G(x)$ were divisible by $\Pi(x)$ say. Then the fundamental form ξ would satisfy the congruence $G(x) \equiv 0 \pmod p$ and hence also the congruence $\Pi^e(x)(\Pi')^{e'}(x) \cdots \equiv 0 \pmod{\mathfrak{p}^{e+1}}$. According to Lemma 5 this is not possible; so the second part of Theorem 33 is established.

These results imply a sequence of important theorems on discriminants.

Theorem 35. *The greatest numerical factor of the discriminant of the fundamental equation is equal to the discriminant of the field.*

Proof. We set

$$\left.\begin{aligned} 1 &= U_{11}\omega_1 + \cdots + U_{1m}\omega_m \\ \xi &= U_{21}\omega_1 + \cdots + U_{2m}\omega_m \\ &\cdots\cdots\cdots \\ \xi^{m-1} &= U_{m1}\omega_1 + \cdots + U_{mm}\omega_m \end{aligned}\right\} \tag{4.1}$$

where $U_{11}, \dots, U_{mm}$ are integer polynomials in $u_1, \dots, u_m$. Let U be the determinant of these m^2 polynomials. If it were the case that all the coefficients of U were divisible by a rational prime number p then it would follow that there were m integer polynomials $V_1, \dots, V_m$ of $u_1, \dots, u_m$ not all congruent to 0 modulo p such that

$$\begin{aligned} V_1U_{11} + \cdots + V_mU_{m1} &\equiv 0 \pmod p \\ &\cdots\cdots\cdots \\ V_1U_{1m} + \cdots + V_mU_{mm} &\equiv 0 \pmod p \end{aligned}$$

identically in $u_1, \ldots, u_m$. From this it would follow that the fundamental form ξ satisfied the congruence

$$V_1 + V_2\xi + \ldots + V_m\xi^{m-1} \equiv 0 \pmod p$$

which is of degree less than m. According to Theorem 34 this cannot happen; so it follows that the determinant U is a rational unit form. Using the multiplication theorem for determinants we deduce from equations (4.1) that

$$\begin{vmatrix} 1 & \xi & \cdots & \xi^{m-1} \\ 1 & \xi' & \cdots & (\xi')^{m-1} \\ & \cdots\cdots & & \\ 1 & \xi^{(m-1)} & \cdots & (\xi^{(m-1)})^{m-1} \end{vmatrix} = U \begin{vmatrix} \omega_1 & \cdots & \omega_m \\ \omega_1' & \cdots & \omega_m' \\ & \cdots\cdots & \\ \omega_1^{(m-1)} & \cdots & \omega_m^{(m-1)} \end{vmatrix}$$

Squaring this relation we obtain $d(\xi) = U^2 d$ or $d(\xi) \simeq d$, where $d(\xi)$ is the discriminant of the fundamental equation and d is the field discriminant.

By solving the equations (4.1) we obtain in addition the following result:

Theorem 36. *Every integer of the field k can be expressed as a rational integral function of degree $m-1$ in the fundamental form ξ. The coefficients of this function are integer polynomials in $u_1, \ldots, u_m$ divided by the rational unit form U (Kronecker (16), Hensel (4)).*

§12. Elements and Different of a Field. Proof of the Theorem on the Divisors of the Discriminant of a Field

Theorem 35 allows us to factorise the field discriminant d as a product of ideal factors. The $m-1$ ideals

$$\begin{aligned} \mathfrak{e}' &= ((\omega_1 - \omega_1'), \ldots, (\omega_m - \omega_m')), \\ \mathfrak{e}'' &= ((\omega_1 - \omega_1''), \ldots, (\omega_m - \omega_m'')), \\ &\cdots\cdots\cdots \\ \mathfrak{e}^{(m-1)} &= ((\omega_1 - \omega_1^{(m-1)}), \ldots, (\omega_m - \omega_m^{(m-1)})) \end{aligned}$$

are called the *elements* of the field k. These are ideals which in general do not belong to the number field k; on the contrary the product $\mathfrak{d} = \mathfrak{e}'\mathfrak{e}'' \ldots \mathfrak{e}^{(m-1)}$ is an ideal of the field k.[1] The elements $\mathfrak{e}', \ldots, \mathfrak{e}^{(m-1)}$ are in fact the contents of

[1] See p. 34, paragraph 2.

the forms $\xi - \xi', \ldots, \xi - \xi^{(m-1)}$ respectively and so we deduce from Theorem 13 that the ideal $\mathfrak{d}$ is the content of the different of the fundamental form, i.e. of

$$\frac{\partial F}{\partial \xi} = (\xi - \xi') \cdots (\xi - \xi^{(m-1)})$$

and this is a form of the field k. The ideal $\mathfrak{d}$ is called the *different*[2] of the field. Its norm is equal to the greatest numerical factor of the discriminant of the fundamental form, and since this (according to Theorem 35) is equal to d we have the following theorem.

Theorem 37. *The norm of the different of a field is equal to its discriminant.*

The congruence

$$\frac{\partial F(x)}{\partial x} \equiv e\Pi^{e-1}\frac{\partial \Pi}{\partial x}(\Pi')^{e'} \cdots + e'\Pi^{e}(\Pi')^{e'-1}\frac{\partial \Pi'}{\partial x} \cdots + \cdots \pmod{\mathfrak{p}}$$

shows further that the different of the field is always divisible by $\mathfrak{p}^{e-1}$ and in the case that the exponent e is prime to p by no higher power of $\mathfrak{p}$. Taking the norm we deduce that the discriminant of the field is always divisible by $p^{f(e-1)+e'(f'-1)+\cdots}$ and when the exponents $e, e', \ldots$ are all prime to p by no higher power of p. This completes the proof of the fundamental Theorem 31 stated at the beginning of Sect. 10.

§13. Determination of Prime Ideals. Constant Numerical Factors of the Rational Unit Form U

The actual calculation of the prime ideals which divide a given rational prime number p can be carried out according to Theorem 33 by factorising the left hand side of the fundamental equation. It is useful to know, however, in what circumstances the parameters $u_1, \ldots, u_m$ in the fundamental equation may be given special values. To this end we introduce the following considerations.

We obtain the discriminants of all the algebraic integers of a field when we let the parameters $u_1, \ldots, u_m$ in $U^2 d$ run through all the rational integers. The greatest common divisor of all these discriminants may not coincide with the field discriminant d for it may very well happen that the rational unit form U may produce for all integral values of $u_1, \ldots, u_m$ a collection of numbers with a fixed divisor other than ± 1. This fact illuminates the significance of the use of the indeterminates $u_1, \ldots, u_m$. We can also easily find a necessary and sufficient condition that the rational prime number p be such a fixed divisor of U; the condition is that U be expressible in the form

[2] Dedekind calls it "das Grundideal".

$$pV + (u_1^p - u_1)V_1 + \cdots + (u_m^p - u_m)V_m$$

where V, V_1, ..., V_m are integer polynomials in u_1, ..., u_m (*Hensel* (1, 2, 5)).

Let us suppose it is possible to give the indeterminates u_1, ..., u_m rational integer values a_1, ..., a_m such that the rational unit form U becomes a number not divisible by p. Then in dealing with the decomposition of the rational prime number p the fundamental equation may be specialised by replacing the form ξ by $\alpha = a_1\omega_1 + \cdots + a_m\omega_m$. In fact, under this hypothesis, it follows easily from Theorem 36 that every integer ω of the field is congruent modulo p to an integer polynomial in α and accordingly an integer polynomial in α of degree less than m cannot be divisible by p unless all its coefficients are divisible by p. Let us denote by $P(x)$, $P'(x)$, ... the polynomials in x alone obtained from $\Pi(x; u_1, \dots, u_m)$, $\Pi'(x; u_1, \dots, u_m)$, ... by the substitutions $u_1 = a_1$, ..., $u_m = a_m$. Then $P(x)$, $P'(x)$, ... are prime polynomials incongruent to one another modulo p and

$$\mathfrak{p} = (p, P(\alpha)), \mathfrak{p}' = (p, P'(\alpha)), \dots .$$

In fact if, after removal of the factor $\mathfrak{p}$, $P(\alpha)$ still contained a prime factor of p, $\mathfrak{p}'$ say, we would have

$$\{P(\alpha)\}^e \{P'(\alpha)\}^{e'-1} \{P''(\alpha)\}^{e''} \cdots \equiv 0 \pmod{p},$$

which, according to what we said above, cannot be the case since the left hand side of this congruence is a polynomial in α of degree less than m.

Conversely we have the easily proved result: If $p = \mathfrak{p}^e(\mathfrak{p}')^{e'} \cdots$ is the decomposition of p in the field k, where $\mathfrak{p}$, $\mathfrak{p}'$, ... are distinct prime ideals of degrees f, f', ... respectively and we can associate to the prime ideals $\mathfrak{p}$, $\mathfrak{p}'$, ... integer polynomials $P(x)$, $P'(x)$, ... in one variable x with degrees f, f', ... respectively which are prime polynomials incongruent to one another modulo p then there exists a number $\alpha = a_1\omega_1 + \cdots + a_m\omega_m$ for which the corresponding value of U is not divisible by p. The non-existence of such mutually incongruent prime polynomials $P(x)$, $P'(x)$, ... thus provides a new necessary and sufficient condition that the prime number p be a fixed numerical factor of U (*Dedekind* (4)).

Each of the two essentially different conditions which we have found in this paragraph can be used to produce numerical examples for number fields in which U actually has fixed numerical factors other than ± 1 (*Dedekind* (4), *Kronecker* (16), *Hensel* (1, 2, 5)).

We should notice, however, that the form U loses the property of containing a fixed numerical factor when we allow the indeterminates u_1, ..., u_m to run through all the algebraic integers of a suitably chosen number field in which all the numbers represented by U in this way have greatest common divisor 1 (*Hensel* (5)).

5. Extension Fields

§14. Relative Norms, Differents and Discriminants

The concepts of norm, different and discriminant can be generalised in an important way.

Let K be a field of degree M which contains all the numbers of a field k of degree m; we say that k is a *subfield* of K and that K is an *extension* of k or a *relative field* with respect to k. Let Θ be a generator of the field K. Among the infinitely many equations with coefficients in k satisfied by Θ let the following equation of degree r

$$\Theta^r + \alpha_1\Theta^{r-1} + \cdots + \alpha_r = 0 \tag{5.1}$$

be of least degree; $\alpha_1, \ldots, \alpha_r$ are then well-determined numbers in k. The degree r is called the *relative degree* of the field K with respect to k; we have $M = rm$. The equation (5.1) of degree r is irreducible in the field k. The remaining $r-1$ roots, $\Theta', \ldots, \Theta^{(r-1)}$ of equation (5.1) are called the *relative conjugate numbers* of Θ and the fields $K', \ldots, K^{(r-1)}$ generated by $\Theta', \ldots, \Theta^{(r-1)}$ respectively are called the *relative conjugate extensions* of K. If A is any number of the field K and we have

$$A = \gamma_1 + \gamma_2\Theta + \cdots + \gamma_r\Theta^{r-1},$$

where $\gamma_1, \ldots, \gamma_r$ are numbers in k, then the numbers

$$\begin{aligned} A' &= \gamma_1 + \gamma_2\Theta' + \cdots + \gamma_r(\Theta')^{r-1}, \\ &\cdots\cdots \\ A^{(r-1)} &= \gamma_1 + \gamma_2\Theta^{(r-1)} + \cdots + \gamma_r(\Theta^{(r-1)})^{r-1} \end{aligned}$$

obtained from A by means of the substitutions $T' = (\Theta : \Theta'), \ldots, T^{(r-1)} = (\Theta : \Theta^{(r-1)})$ respectively are called the *relative conjugate numbers* of A. If we apply the substitution T' to all the numbers of an ideal $\mathfrak{J}$ the ideal $\mathfrak{J}'$

which we obtain is called the *relative conjugate ideal* of $\mathfrak{J}$ corresponding to the substitution T'.

The product of a number A with its relative conjugate numbers

$$N_k(A) = AA' \cdots A^{(r-1)}$$

is called the *relative norm of the number A* with respect to the field k. The relative norm $N_k(A)$ is a number in k. If $\mathfrak{J} = (A_1, \dots, A_S)$ is any ideal of K then the product of $\mathfrak{J}$ with all its relative conjugate ideals

$$N_k(\mathfrak{J}) = \mathfrak{J}\mathfrak{J}' \cdots \mathfrak{J}^{(r-1)}$$

is called the *relative norm of the ideal* $\mathfrak{J}$. The relative norm $N_k(\mathfrak{J})$ is an ideal of the field k. For if $U_1, \dots, U_S$ are indeterminates the coefficients of the expression

$$(A_1U_1 + \dots + A_SU_S)(A_1'U_1 + \dots + A_S'U_S) \cdots (A_1^{(r-1)}U_1 + \dots + A_S^{(r-1)}U_S)$$

are integers of k whose greatest common divisor must, according to Theorem 13, coincide with the above product of ideals.

Let $\alpha_1, \dots, \alpha_s$ be any numbers of k and $\mathfrak{i} = (\alpha_1, \dots, \alpha_s)$ the ideal of k which they determine; these numbers also determine an ideal $\mathfrak{J} = (\alpha_1, \dots, \alpha_s)$ of K. This ideal is not to be thought of as different from $\mathfrak{i}$. Conversely, an ideal $\mathfrak{J} = (A_1, \dots, A_S)$ of K is to be regarded as an ideal $\mathfrak{i}$ of k precisely when $\mathfrak{J}$ can be represented as the greatest common divisor of certain integers $\alpha_1, \dots, \alpha_s$ of the field k. That we are entitled in these circumstances to regard $(\alpha_1, \dots, \alpha_s)$ both as an ideal of k and as an ideal of K is shown by the following theorem: if $\alpha_1, \dots, \alpha_s$ and $\alpha_1^*, \dots, \alpha_{s^*}^*$ are integers in k such that the two ideals $\mathfrak{J} = (\alpha_1, \dots, \alpha_s)$ and $\mathfrak{J}^* = (\alpha_1^*, \dots, \alpha_{s^*}^*)$ of K coincide then the ideals $\mathfrak{i} = (\alpha_1, \dots, \alpha_s)$ and $\mathfrak{i}^* = (\alpha_1^*, \dots, \alpha_{s^*}^*)$ of k also coincide. In fact it follows from the hypothesis that if α^* is one of the numbers $\alpha_1^*, \dots, \alpha_{s^*}^*$ then we have an equation of the form $\alpha^* = A_1\alpha_1 + \cdots + A_s\alpha_s$, where $A_1, \dots, A_s$ are integers in K; if we take relative norms of both sides of this equation we see that in the field k the number α^{*r} must be divisible by $\mathfrak{i}^r$; hence α^* must be divisible in k by $\mathfrak{i}$ and so $\mathfrak{i}^*$ must be divisible by $\mathfrak{i}$. By the same argument $\mathfrak{i}$ must be divisible by $\mathfrak{i}^*$; hence $\mathfrak{i} = \mathfrak{i}^*$.

The expression

$$\Delta_k(A) = (A - A')(A - A'') \cdots (A - A^{(r-1)})$$

represents a number of the field K; it is called the *relative different of the number A* with respect to the field k. The expression

$$D_k(A) = (A - A')^2(A - A'')^2 \cdots (A^{(r-2)} - A^{(r-1)})^2$$

is called the *relative discriminant of the number A*. Up to its sign the relative discriminant of a number is equal to the relative norm of its relative different: we have in fact $D_k(A) = (-1)^{r(r-1)/2} N_k(\Delta_k(A))$.

Let $\Omega_1, \ldots, \Omega_M$ form a basis for the field K. Then the ideal

$$\mathfrak{D}_k = \mathfrak{E}'\mathfrak{E}'' \cdots \mathfrak{E}^{(r-1)}$$

formed by multiplying the $r-1$ *elements*

$$\begin{aligned} \mathfrak{E}' &= ((\Omega_1 - \Omega_1'), \ldots, (\Omega_M - \Omega_M')), \\ &\ldots\ldots\ldots \\ \mathfrak{E}^{(r-1)} &= ((\Omega_1 - \Omega_1^{(r-1)}), \ldots, (\Omega_M - \Omega_M^{(r-1)})) \end{aligned}$$

is called the *relative different of the field* K with respect to k. If

$$\Xi = \Omega_1 U_1 + \cdots + \Omega_M U_M$$

is the fundamental form of K then the relative different of Ξ is

$$\Delta_k(\Xi) = (\Xi - \Xi') \cdots (\Xi - \Xi^{(r-1)}).$$

The coefficients of this form are numbers of the field K and since, according to Theorem 13, the greatest common divisor of these is the relative different $\mathfrak{D}_k$ it follows that $\mathfrak{D}_k$ is an ideal of the field K.

The square of the greatest common divisor of all $r \times r$ subdeterminants of the matrix

$$\begin{bmatrix} \Omega_1 & \Omega_2 & \ldots & \Omega_M \\ \Omega_1' & \Omega_2' & \ldots & \Omega_M' \\ & & \ldots\ldots & \\ \Omega_1^{(r-1)} & \Omega_2^{(r-1)} & \ldots & \Omega_M^{(r-1)} \end{bmatrix} \tag{5.2}$$

is called the *relative discriminant* D_k *of the field* K with respect to k; it is easily seen to be an ideal of the field k.

§15. Properties of the Relative Different and Discriminant

We have the following theorems concerning the concepts we have just defined (*Hilbert* (4)).

Theorem 38. *The relative discriminant of a field K with respect to a subfield k is equal to the relative norm of the relative different of K, i.e.*

$$D_k = N_k(\mathfrak{D}_k).$$

Proof. The relative norm of the relative different of the fundamental form Ξ is given by

$$\begin{aligned} N_k(\Delta_k(\Xi)) &= \pm(\Xi-\Xi')^2(\Xi-\Xi'')^2\cdots(\Xi^{(r-2)}-\Xi^{(r-1)})^2 \\ &= \pm\begin{vmatrix} 1 & \Xi & \cdots & \Xi^{r-1} \\ 1 & \Xi' & \cdots & (\Xi')^{r-1} \\ & & \cdots\cdots & \\ 1 & \Xi^{(r-1)} & \cdots & (\Xi^{(r-1)})^{r-1} \end{vmatrix}^2 \end{aligned}$$

On the other hand the square of the determinant on the right hand side is a form of the field K whose content is equal to the relative discriminant D_k. To see this we express the entries of the above determinant as linear combinations of the basis elements $\Omega_1, \ldots, \Omega_M$ and their respective conjugates, with coefficients which are integer polynomials in $U_1, \ldots, U_M$; then we recognise that the square of the determinant has all its coefficients divisible by D_k. Conversely, using Theorem 36, we see that the product of each $r \times r$ subdeterminant of the matrix (5.2) by the r-th power of a certain rational unit form in the parameters $U_1, \ldots, U_M$ is divisible by the product of differences

$$(\Xi-\Xi')(\Xi-\Xi'')\cdots(\Xi^{(r-2)}-\Xi^{(r-1)}).$$

It follows that $N_k(\Delta_k(\Xi)) \simeq D_k$.

Theorem 39. *Let D and d be the discriminants of the extension field K and the subfield k respectively and let $n(D_k)$ be the norm of the relative discriminant D_k considered as an ideal of k. Then*

$$D = \pm d^r n(D_k).$$

Proof. Let $\xi = \omega_1 u_1 + \cdots + \omega_m u_m$ be the fundamental form of the field k. Then Ξ satisfies an equation in X of degree r having the form

$$\Phi(\mathsf{X}, \xi) = \Phi_0 \mathsf{X}^r + \Phi_1 \mathsf{X}^{r-1} + \cdots + \Phi_r = 0$$

where $\Phi_1, \ldots, \Phi_r$ are integer polynomials in ξ and the indeterminates $u_1, \ldots, u_m, U_1, \ldots, U_M$, while Φ_0 is a rational unit form of the indeterminates $u_1, \ldots, u_m$. The remaining roots of the above equation are $\mathsf{X} = \Xi', \ldots, \Xi^{(r-1)}$. Next let $\xi^{(h)}$ be one of the $m-1$ fundamental forms conjugate to ξ; we denote the roots of the r-th degree equation $\Phi(X, \xi^{(h)}) = 0$ by $\Xi_{(h)}, \Xi'_{(h)}, \ldots, \Xi^{(r-1)}_{(h)}$. Since ξ satisfies an equation of degree m it is obvious that the product of each power of Ξ by a power of Φ_0 is an integer polynomial in ξ and Ξ of degree in ξ not greater than $m-1$ and in Ξ not greater than $r-1$ with coefficients which are functions of the parameters $u_1, \ldots, u_m, U_1, \ldots, U_M$ with integer coefficients. Hence it follows that the product of the discriminant of the fundamental form Ξ by a power of Φ_0 is divisible by the square of the $mr \times mr$ determinant $\Delta =$

$$\begin{vmatrix} 1 & \Xi & .. & \Xi^{r-1} & \xi & \xi\Xi & .. & \xi\Xi^{r-1}\ldots \\ & & & \ldots & \xi^{m-1} & \xi^{m-1}\Xi & .. & \xi^{m-1}\Xi^{r-1} \\ 1 & \Xi' & .. & (\Xi')^{r-1} & \xi & \xi\Xi' & .. & \xi(\Xi')^{r-1}\ldots \\ & & & \ldots & \xi^{m-1} & \xi^{m-1}\Xi' & .. & \xi^{m-1}(\Xi')^{r-1} \\ & & & & \ldots\ldots & & & \\ 1 & \Xi^{(r-1)} & .. & (\Xi^{(r-1)})^{r-1} & \xi & \xi\Xi^{(r-1)} & .. & \xi(\Xi^{(r-1)})^{r-1}\ldots \\ & & & \ldots & \xi^{m-1} & \xi^{m-1}\Xi^{(r-1)} & .. & \xi^{m-1}(\Xi^{(r-1)})^{r-1} \\ & & & & \ldots\ldots & & & \end{vmatrix}$$

where we have shown only the first r rows of the determinant. The remaining $(m-1)r$ rows are obtained when we attach to all the symbols ξ the indices $(h) = (1), \ldots, (m-1)$ as superscripts and the same indices as subscripts to all the symbols Ξ.

If we now express all the elements of Δ as linear combinations of the numbers $\Omega_1, \ldots, \Omega_M$ of the basis and their conjugates we have the identity

$$\Delta = \begin{vmatrix} \Omega_1 & \cdots & \Omega_M \\ \Omega_1' & \cdots & \Omega_M' \\ & \cdots\cdots & \\ \Omega_1^{(M-1)} & \cdots & \Omega_M^{(M-1)} \end{vmatrix} F$$

where F is an integer polynomial in the parameters $u_1, \ldots, u_m, U_1, \ldots, U_M$. It follows that the numerical factor of the square of Δ is divisible by D. Since, however, the numerical factor of the discriminant of Ξ is D (according to Theorem 35) it follows from the preceding discussion that conversely D is divisible by the numerical factor of the square of Δ. Hence the numerical factor of Δ^2 is precisely D.

From elementary theorems in the theory of determinants we have the identity

$$\Delta = \begin{vmatrix} 1 & \xi & \cdots & \xi^{m-1} \\ 1 & \xi' & \cdots & (\xi')^{m-1} \\ & & \cdots\cdots & \\ 1 & \xi^{(m-1)} & \cdots & (\xi^{(m-1)})^{m-1} \end{vmatrix}^r \Pi$$

where

$$\Pi = \begin{vmatrix} 1 & \Xi & \cdots & \Xi^{r-1} \\ 1 & \Xi' & \cdots & (\Xi')^{r-1} \\ & & \cdots\cdots & \\ 1 & \Xi^{(r-1)} & \cdots & (\Xi^{(r-1)})^{r-1} \end{vmatrix} \begin{vmatrix} 1 & \Xi_{(1)} & \cdots & \Xi_{(1)}^{r-1} \\ 1 & \Xi_{(1)}' & \cdots & (\Xi_{(1)}')^{r-1} \\ & & \cdots\cdots & \\ 1 & \Xi_{(1)}^{(r-1)} & \cdots & (\Xi_{(1)}^{(r-1)})^{r-1} \end{vmatrix} \cdots$$

$$\cdots \begin{vmatrix} 1 & \Xi_{(m-1)} & \cdots & \Xi_{(m-1)}^{r-1} \\ 1 & \Xi_{(m-1)}' & \cdots & (\Xi_{(m-1)}')^{r-1} \\ & & \cdots\cdots & \\ 1 & \Xi_{(m-1)}^{(r-1)} & \cdots & (\Xi_{(m-1)}^{(r-1)})^{r-1} \end{vmatrix}$$

and from this Theorem 39 follows immediately.

Theorem 39 which we have just proved shows not only that the discriminant of a field is divisible by the discriminant of each of its subfields but also gives a certain power of the latter which divides the discriminant of the extension field and also reveals the simple significance of the remaining factor.

§16. Decomposition of an Element of a Field k in an Extension K. Theorem on the Different of the Extension K

Theorem 40. *Each element of the subfield k is equal to the product of r elements of the extension K; we have in fact*

$$\begin{aligned}\xi - \xi^{(h)} &\simeq (\Xi - \Xi_{(h)})(\Xi - \Xi'_{(h)}) \cdots (\Xi - \Xi_{(h)}^{(r-1)}) \\ &\simeq (\Xi - \Xi_{(h)})(\Xi' - \Xi_{(h)}) \cdots (\Xi^{(r-1)} - \Xi_{(h)}).\end{aligned}$$

Proof. Let

$$F(\mathsf{X}) = \mathsf{X}^M + F_1\mathsf{X}^{m-1} + \cdots + F_M = 0$$

be the fundamental equation of degree M of the field K, where $F_1, \ldots, F_M$ are integer polynomials in $U_1, \ldots, U_M$. Then we have

$$\Phi_0^m F(\mathsf{X}) = \Phi(\mathsf{X}, \xi)\Phi(\mathsf{X}, \xi') \cdots \Phi(\mathsf{X}, \xi^{(m-1)})$$

identically in X.

Since $\Phi(\Xi, \xi) = 0$ it follows that the different of the fundamental form Ξ is represented by the formula

$$\Delta(\Xi) = \frac{\partial F(\Xi)}{\partial \Xi} = \frac{1}{\Phi_0^m}\frac{\partial \Phi(\Xi, \xi)}{\partial \Xi}\Phi(\Xi, \xi') \cdots \Phi(\Xi, \xi^{(m-1)}).$$

Now for $h = 1, 2, \ldots, m-1$ we have on the one hand

$$\Phi(\Xi, \xi^{(h)}) = \Phi_0(\Xi - \Xi_{(h)})(\Xi - \Xi'_{(h)}) \cdots (\Xi - \Xi_{(h)}^{(r-1)}) \tag{5.3}$$

and on the other hand

$$\Phi(\Xi, \xi^{(h)}) = \Phi(\Xi, \xi^{(h)}) - \Phi(\Xi, \xi) = (\xi - \xi^{(h)})G^{(h)} \tag{5.4}$$

where $G^{(h)}$ is an integral algebraic form. From this it follows that

$$\Phi_0^m \frac{\partial F(\Xi)}{\partial \Xi} = \frac{\partial \Phi(\Xi, \xi)}{\partial \Xi}(\xi - \xi') \cdots (\xi - \xi^{(m-1)})G' \cdots G^{(m-1)}.$$

Since

$$\frac{1}{\Phi_0}\frac{\partial \Phi(\Xi, \xi)}{\partial \Xi}$$

represents the relative different of Ξ we deduce from the last result, using Theorem 13, that

$$\mathfrak{D} = \mathfrak{D}_k \mathfrak{d} \mathfrak{J} \tag{5.5}$$

where $\mathfrak{D}$ is the different of K, $\mathfrak{D}_k$ the relative different of K with respect to k, $\mathfrak{d}$ the different of k and $\mathfrak{J}$ the ideal which is the content of the form $G' \ldots G^{(m-1)}$. Taking the norm we have $D = n(D_k)d^r N(\mathfrak{J})$ and consequently, by Theorem 39, $N(\mathfrak{J}) = 1$, so that $\mathfrak{J} = 1$. The forms $G', \ldots, G^{(m-1)}$ are thus all unit forms and Theorem 40 follows from equations (5.3) and (5.4).

Theorem 40 gives us the decomposition of the elements of the field k in the extension K; it is the foundation of the theory of discriminants. Equation (5.5) yields in addition the following important fact.

Theorem 41. *The different $\mathfrak{D}$ of the field K is equal to the product of the relative different $\mathfrak{D}_k$ of K with respect to the subfield k and the different $\mathfrak{d}$ of the field k, i.e.*

$$\mathfrak{D} = \mathfrak{D}_k \mathfrak{d}.$$

According to this theorem the behaviour of the different when we move from a field to an extension is remarkably simple: we obtain the different of the higher field when we multiply the different of the lower field by the corresponding relative different.

6. Units of a Field

§17. Existence of Conjugates with Absolute Values Satisfying Certain Inequalities

In Chapter 2 we gave a full treatment of the laws concerning the divisibility of numbers in an algebraic number field. We now pass on to develop some additional results in which the concept of absolute value plays an essential rôle. The most important tool for this investigation is the following result (*Minkowski* (3)).

Lemma 6. *Let*

$$\begin{aligned} f_1 &= a_{11}u_1 + \cdots + a_{1m}u_m, \\ &\cdots\cdots\cdots \\ f_m &= a_{m1}u_1 + \cdots + a_{mm}u_m \end{aligned}$$

be m homogeneous linear forms in $u_1, \ldots, u_m$ with arbitrary real number coefficients $a_{11}, \ldots, a_{mm}$ with determinant 1. Then we can find rational integer values for $u_1, \ldots, u_m$, not all zero, such that the absolute values of the forms $f_1, \ldots, f_m$ are all ≤ 1.

We can recast the result slightly to obtain the following.

Lemma 7. *Let $f_1, \ldots, f_m$ be homogeneous linear forms in $u_1, \ldots, u_m$ with positive determinant A; let $\kappa_1, \ldots, \kappa_m$ be positive constants whose product is A. Then we can find rational integer values for $u_1, \ldots, u_m$, not all zero, such that the absolute values of the m forms satisfy the conditions*

$$|f_1| \leq \kappa_1, \ldots, |f_m| \leq \kappa_m.$$

We remark that in this chapter we depart from the notation used in the earlier chapters and denote the field k and its conjugates by $k^{(1)} = k$, $k^{(2)}$, $\ldots$, $k^{(m)}$ and correspondingly the conjugates of the basis numbers $\omega_1, \ldots,$ ω_m in $k^{(s)}$ are denoted by $\omega_1^{(s)}, \ldots, \omega_m^{(s)}$.

We apply Lemma 7 in proving the following fact.

Theorem 42. *Let $\kappa_1, \ldots, \kappa_m$ be arbitrary positive real constants whose product is $|\sqrt{d}|$ satisfying the condition that if $k^{(s)}$ and $k^{(s')}$ are conjugate imaginary fields then $\kappa_s = \kappa_{s'}$. Then there exists a nonzero integer ω in the field k such that*

$$|\omega^{(1)}| \leq \kappa_1, \ldots, |\omega^{(m)}| \leq \kappa_m.$$

Proof. We associate with each of the fields $k^{(1)}, \ldots, k^{(m)}$ a linear form, according to the following prescription. If $k^{(r)}$ is a real field we associate with it the linear form

$$f_r = \omega_1^{(r)} u_1 + \cdots + \omega_m^{(r)} u_m$$

while if $k^{(s)}$ is an imaginary field and $k^{(s')}$ its conjugate imaginary field we associate with $k^{(s)}$ and $k^{(s')}$ the linear forms

$$\left.\begin{aligned} f_s &= \frac{1}{\sqrt{2}}\{(\omega_1^{(s)} + \omega_1^{(s')})u_1 + \cdots + (\omega_m^{(s)} + \omega_m^{(s')})u_m\} \\ f_{s'} &= \frac{1}{i\sqrt{2}}\{(\omega_1^{(s)} - \omega_1^{(s')})u_1 + \cdots + (\omega_m^{(s)} - \omega_m^{(s')})u_m\} \end{aligned}\right\} \tag{6.1}$$

respectively, which both have real coefficients. The determinant of the m forms $f_1, \ldots, f_m$ has absolute value $|\sqrt{d}|$. The conclusion of the theorem then follows immediately from Lemma 7 when we bear in mind that for each pair of conjugate imaginary fields $k^{(s)}, k^{(s')}$ we have

$$f_s^2 + f_{s'}^2 = 2|\omega_1^{(s)} u_1 + \cdots + \omega_m^{(s)} u_m|^2.$$

The following result follows easily.

Theorem 43. *For a given degree m and a given positive constant κ there exist only finitely many algebraic integers of degree m which, along with their conjugates, have absolute value less than κ.*

Proof. The m rational integer coefficients of the equation which such an algebraic integer satisfies must all be less in absolute value than a bound which depends only on m and κ. It follows that there are only finitely many such integers.

§18. Absolute Value of the Field Discriminant

We prove the following two theorems.

Theorem 44. *The discriminant d of a number field k is always different from ± 1 (Minkowski (1, 2, 3)).*

Theorem 45. *There are only finitely many fields of degree m with given discriminant d (Hermite (1, 2), Minkowski (3)).*

The following lemma is of use in proving these theorems.

Lemma 8. *If $f_1, \ldots, f_m$ are the m real linear forms in the indeterminates $u_1, \ldots, u_m$ defined in equations (6.1) then there exists a nonzero integer $\alpha = a_1\omega_1 + \ldots + a_m\omega_m$ in k for which the absolute values of the forms with $u_1 = a_1, \ldots, u_m = a_m$ satisfy the inequalities*

$$|f_1| \leq |\sqrt{d}|, |f_2| \leq 1, |f_3| \leq 1, \ldots, |f_m| \leq 1. \tag{6.2}$$

Proof. According to Theorem 43 there can be only a finite number of integers $\alpha, \alpha_1, \alpha_2, \ldots$ in k which satisfy the conditions

$$|f_1| \leq |\sqrt{d}| + 1, |f_2| \leq 1, \ldots, |f_m| \leq 1.$$

Let α be the integer among $\alpha, \alpha_1, \alpha_2, \ldots$ for which $|f_1|$ takes the smallest value; and let this smallest value be φ. If there are in fact no such numbers, set $\varphi = |\sqrt{d}|+1$. If $\varphi \leq |\sqrt{d}|$ then the result of Lemma 8 follows immediately. If, on the other hand, $\varphi > |\sqrt{d}|$ we find a positive real number ε such that $(1+\varepsilon)^{m-1}|\sqrt{d}| < \varphi$. According to Lemma 7 there exists a set of rational integers $u_1, \ldots, u_m$, not all zero, such that

$$|f_1| \leq (1+\varepsilon)^{m-1}|\sqrt{d}|, |f_2| \leq \frac{1}{1+\varepsilon}, \ldots, |f_m| \leq \frac{1}{1+\varepsilon}$$

and consequently

$$|f_1| < \varphi, |f_2| < 1, \ldots, |f_m| < 1.$$

But this contradicts our choice of α.

Now to prove both Theorems 44 and 45 we proceed as follows. If $k = k^{(1)}$ is a real field the form f_1 is uniquely determined. If, however, $k^{(1)}$ is an imaginary field and $k^{(2)}$ is its conjugate there are two possible choices for the form f_1; we set

$$f_1 = \frac{1}{i\sqrt{2}}\{(\omega_1^{(1)} - \omega_1^{(2)})u_1 + \cdots + (\omega_m^{(1)} - \omega_m^{(2)})u_m\}.$$

The order of the remaining forms $f_2, \ldots, f_m$ is immaterial. Lemma 8 shows that there exists an integer α which satisfies the conditions (6.2). On the other hand

$$\prod_{(r)} |f_r| \prod_{s,s'} \frac{f_s^2 + f_{s'}^2}{2} = |n(\alpha)|,$$

where the first product is taken over all forms f_r and the second over all pairs f_s, $f_{s'}$. Since $|n(\alpha)| \geq 1$ it follows that $|f_1| > 1$ and hence that $|\sqrt{d}\,| > 1$. Thus Theorem 44 is established.

At the same time it follows from the inequalities $|f_1| > 1$, $|f_2| < 1, \ldots,$ $|f_m| < 1$ that α is a number of the field $k = k^{(1)}$ which is distinct from all its conjugates; so the different $\delta(\alpha)$ is nonzero. It follows, in accordance with a remark in Sect. 3, that α is a generator of the field k. Since d is a prescribed number it follows from Theorem 43 that there are only finitely many algebraic integers of degree m which, together with their conjugates, satisfy conditions (6.2). The assertion of Theorem 45 follows immediately.

Theorem 44 reveals a property which lies very deep in the nature of algebraic numbers, namely that the discriminant of every number field must be divisible by at least one prime number.

If, instead of the result we quoted in Lemma 6 and used as basis for all our investigation, we were to use another, sharper, result of Minkowski, the same line of argument would lead to the result that the absolute value of the discriminant of a field of degree m is always greater than

$$\left(\frac{\pi}{4}\right)^{2r_2} \left(\frac{m^m}{m!}\right)^2$$

and hence is greater than

$$\left(\frac{\pi}{4}\right)^{2r_2} \frac{e^{2m-\frac{1}{6m}}}{2\pi m},$$

where r_2 is the number of conjugate imaginary pairs among the m conjugate fields $k^{(1)}, \ldots, k^{(m)}$ (*Minkowski* (1, 2, 3)).

This last result, used in a corresponding way, shows again that among the fields of all possible degrees there can be only finitely many with a prescribed discriminant d.

From these results we deduce also the following fact which is important for Chapter 7 (*Minkowski* (1, 3)).

Theorem 46. *For each ideal $\mathfrak{a}$ of a field k there exists a nonzero integer α in k which is divisible by $\mathfrak{a}$ and whose norm satisfies the condition*

$$|n(\alpha)| \leq |n(\mathfrak{a})\sqrt{d}\,|.$$

Proof. Let

$$\begin{aligned}\iota_1 &= a_{11}\omega_1 + \cdots + a_{1m}\omega_m\\ &\cdots\cdots\cdots\\ \iota_m &= a_{m1}\omega_1 + \cdots + a_{mm}\omega_m\end{aligned}$$

be the m basis numbers of the ideal $\mathfrak{a}$. Then we can construct from these, in precisely the same way as we did with $\omega_1, \ldots, \omega_m$, m linear forms $f_1, \ldots, f_m$ with real coefficients. The determinant of these m forms is equal in absolute value to

$$\begin{vmatrix} \iota_1^{(1)} & \cdots & \iota_m^{(1)} \\ \cdots & \cdots & \cdots \\ \iota_1^{(m)} & \cdots & \iota_m^{(m)} \end{vmatrix} = \begin{vmatrix} a_{11} & \cdots & a_{1m} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mm} \end{vmatrix} \begin{vmatrix} \omega_1^{(1)} & \cdots & \omega_m^{(1)} \\ \cdots & \cdots & \cdots \\ \omega_1^{(m)} & \cdots & \omega_m^{(m)} \end{vmatrix}$$

and consequently, according to Theorem 19, has absolute value $|n(\mathfrak{a})\sqrt{d}\,|$. Now associate with the forms $f_1, \ldots, f_m$ real positive constants $\kappa_1, \ldots, \kappa_m$ whose product is $|n(\mathfrak{a})\sqrt{d}\,|$ and which are such that $\kappa_s = \kappa_{s'}$ when $k^{(s)}$ and $k^{(s')}$ are conjugate imaginary fields. Theorem 46 then follows at once from Theorem 42.

§19. Theorem on the Existence of Units

The most important foundation stone for the deeper study of algebraic integers is the following fundamental theorem on the units of a field k (*Dirichlet* (13, 14, 16), *Dedekind* (1), *Kronecker* (18), (20), *Minkowski* (3)).

An integer ε of a field k whose reciprocal $1/\varepsilon$ is also an integer is called a *unit* of k. The norm of a unit is ± 1; conversely, every integer in k whose norm is ± 1 is a unit of k.

Theorem 47. *Suppose that among the m conjugate fields $k^{(1)}, \ldots, k^{(m)}$ there are r_1 real fields and $r_2 = \frac{1}{2}(m - r_1)$ pairs of conjugate imaginary fields. Then $k = k^{(1)}$ contains a set of $r = r_1 + r_2 - 1$ units $\varepsilon_1, \ldots, \varepsilon_r$ such that every unit ε of k can be uniquely expressed in the form*

$$\varepsilon = \rho\varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}$$

where $a_1, \ldots, a_r$ are rational integers and ρ is a root of unity in k.

In preparation for the proof of this theorem we arrange the m conjugate fields $k^{(1)}, \ldots, k^{(m)}$ in a special way, as follows. First we take the r_1 real fields $k^{(1)}, \ldots, k^{(r_1)}$; then we choose one field from each of the r_2 pairs of conjugate imaginary fields, calling them $k^{(r_1+1)}, \ldots, k^{(r_1+r_2)}$; we follow these

with their conjugates $k^{(r_1+r_2+1)}, \ldots, k^{(m)}$. Now we introduce m linear forms in m real variables $u_1, \ldots, u_m$, namely

$$\xi_s = \omega_1^{(s)} u_1 + \cdots + \omega_m^{(s)} u_m \quad (s = 1, 2, \ldots, m)$$

and write $\xi = \xi_1$. If $\xi_1, \ldots, \xi_m$ are all nonzero we write, in the case where $k^{(s)}$ is a real field,

$$\log|\xi_s| = l_s(\xi)$$

and, when $k^{(s)}$, $k^{(s')}$ are conjugate imaginary fields,

$$\begin{aligned} \log(\xi_s) &= \tfrac{1}{2} l_s(\xi) - i l_{s'}(\xi) \\ \log(\xi_{s'}) &= \tfrac{1}{2} l_s(\xi) + i l_{s'}(\xi) \end{aligned}$$

where $l_1(\xi), \ldots, l_m(\xi)$ are all real numbers and in particular the values $l_{s'}(\xi)$ satisfy the inequalities

$$0 \le l_{s'}(\xi) < 2\pi.$$

In this way $l_1(\xi), \ldots, l_m(\xi)$ are uniquely determined real functions of the real variables $u_1, \ldots, u_m$; we call them the *logarithms of the form* ξ. If $ln(\xi)$ denotes the real part of the logarithm of $n(\xi)$ we have

$$l_1(\xi) + \cdots + l_{r+1}(\xi) = ln(\xi).$$

If $u_1, \ldots, u_m$ are rational integers, not all zero, then $\xi = \xi_1$ represents a nonzero integer α of the field $k = k^{(1)}$. The numbers $l_1(\xi), \ldots, l_m(\xi)$ are then uniquely determined by the number α and are called the *logarithms of the number* α. If ε is a unit of the field k then, since $n(\varepsilon) = \pm 1$, we have

$$l_1(\varepsilon) + l_2(\varepsilon) + \cdots + l_{r+1}(\varepsilon) = 0.$$

Conversely, the real variables $u_1, \ldots, u_m$ are determined by the logarithms $l_1(\xi), \ldots, l_m(\xi)$ in a 2^{r_1}-valued way, since the r_1 real values $\xi_1, \ldots, \xi_{r_1}$ are determined by means of the logarithms only in absolute value, while the remaining conjugate pairs of imaginary values are completely determined.

In order to calculate the functional determinant of this dependence relation, which we shall use later, we introduce the following notation: if $f_1, \ldots, f_m$ are m arbitrary functions of the variables $x_1, \ldots, x_m$ then the functional determinant of $f_1, \ldots, f_m$ with respect to $x_1, \ldots, x_m$ is denoted by

$$\frac{f_1, \ldots, f_m}{x_1, \ldots, x_m}.$$

Then for the absolute values we have the formulæ

$$\left|\frac{u_1, \ldots, u_m}{\xi_1, \ldots, \xi_m}\right| = \frac{1}{|\sqrt{d}\,|}, \qquad \left|\frac{\xi_1, \ldots, \xi_m}{l_1(\xi), \ldots, l_m(\xi)}\right| = |\,\xi_1, \ldots, \xi_m| = |\,n(\xi)|$$

and by multiplying these we obtain the value of

$$\left|\frac{u_1, \ldots, u_m}{l_1(\xi), \ldots, l_m(\xi)}\right|.$$

In what follows we shall be concerned mainly with the first r logarithms $l_1, \ldots, l_r$ of a form ξ or a number α. For the first r logarithms of forms ξ, η or of numbers α, β, we have obviously the equations

$$\left.\begin{array}{lcl} l_s(\xi\eta) & = & l_s(\xi) + l_s(\eta) \\ l_s(\alpha\beta) & = & l_s(\alpha) + l_s(\beta) \end{array}\right\} \quad (s = 1, \ldots, r).$$

We prove now the following fact.

Lemma 9. *Let $\gamma_1, \ldots, \gamma_r$ be arbitrary real constants, not all zero. Then there exists a unit ε in k such that*

$$\gamma_1 l_1(\varepsilon) + \cdots + \gamma_r l_r(\varepsilon) \neq 0.$$

Proof. If ω is any nonzero integer in k we write for short

$$L(\omega) = \gamma_1 l_1(\omega) + \cdots + \gamma_r l_r(\omega);$$

we determine an arbitrary set of r real numbers $\lambda_1, \ldots, \lambda_r$ such that $\gamma_1\lambda_1 + \ldots + \gamma_r\lambda_r = 1$ and set

$$\Lambda_1 = e^{\lambda_1 t}, \ldots, \Lambda_{r_1} = e^{\lambda_{r_1} t}, \Lambda_{r_1+1} = e^{\frac{1}{2}\lambda_{r_1+1} t}, \ldots, \Lambda_r = e^{\frac{1}{2}\lambda_r t},$$

where t is an arbitrary real parameter.

There are now two cases to consider, according as the m conjugate fields $k^{(1)}, \ldots, k^{(m)}$ are all real or not. In the first case we associate with the $r = m - 1$ fields $k^{(1)}, \ldots, k^{(r)}$ the numbers $\Lambda_1, \ldots, \Lambda_r$ and with the final remaining field $k^{(m)}$ the constant

$$\Lambda_m = \frac{|\sqrt{d}\,|}{\Lambda_1 \cdots \Lambda_{m-1}}.$$

In the second case we again associate with the fields $k^{(1)}, \ldots, k^{(r)}$ the numbers $\Lambda_1, \ldots, \Lambda_r$; with the imaginary field $k^{(r+1)}$ we associate the number

$$\Lambda_{r+1} = \left|\left\{\frac{\sqrt{d}}{\Lambda_1 \cdots \Lambda_{r_1}\Lambda_{r_1+1}^2 \cdots \Lambda_r^2}\right\}^{\frac{1}{2}}\right|;$$

finally we associate with the remaining $m - r - 1$ imaginary fields $k^{(r+2)}, \ldots, k^{(m)}$ respectively the same constants as are already associated with their conjugate imaginary fields; we denote the corresponding numbers by $\Lambda_{r+2}, \ldots, \Lambda_m$. In both cases we have the product

$$\Lambda_1 \cdots \Lambda_m = |\sqrt{d}\,|$$

and so the constants $\Lambda_1, \ldots, \Lambda_m$ satisfy the conditions imposed on $\kappa_1, \ldots, \kappa_m$ in Theorem 42.

It follows then from Theorem 42 that there is a nonzero number α in the field k such that

$$|\alpha^{(1)}| \leq \Lambda_1, \ldots, |\alpha^{(m)}| \leq \Lambda_m \tag{6.3}$$

and consequently $|n(\alpha)| \leq |\sqrt{d}\,|$. Since $|n(\alpha)| \geq 1$ we have, for all $s = 1, 2, \ldots, m$,

$$|\alpha^{(s)}| \geq 1/|\alpha^{(1)}| \ldots |\alpha^{(s-1)}||\alpha^{(s+1)}| \ldots |\alpha^{(m)}|;$$

bearing in mind the relations

$$\frac{1}{|\alpha^{(1)}|} \geq \frac{1}{\Lambda_1}, \ldots, \frac{1}{|\alpha^{(m)}|} \geq \frac{1}{\Lambda_m}$$

and

$$\Lambda_1 \cdots \Lambda_m = |\sqrt{d}\,|$$

we deduce that

$$|\alpha^{(s)}| \geq \frac{\Lambda_s}{|\sqrt{d}\,|}. \tag{6.4}$$

From the two inequalities (6.3) and (6.4) we deduce that

$$\lambda_s t \geq l_s(\alpha) \geq \lambda_s t - 2\delta \qquad (s = 1, \ldots, r)$$

where δ is the real value of $\log|\sqrt{d}\,|$. Thus

$$0 \leq |l_s(\alpha) - \lambda_s t| \leq 2\delta \qquad (s = 1, \ldots, r).$$

From this we deduce that the form

$$\gamma_1\{l_1(\alpha) - \lambda_1 t\} + \cdots + \gamma_r\{l_r(\alpha) - \lambda_r t\} = L(\alpha) - t$$

lies between certain finite bounds δ_1 and δ_2 with $\delta_2 > \delta_1$, which depend only on d and $\gamma_1, \ldots, \gamma_r$ and not on the value of the parameter t.

Let Δ be a real number such that $\Delta > \delta_2 - \delta_1$. Taking $t = 0, \Delta, 2\Delta, 3\Delta, \ldots$ in turn and applying the procedure described above, we obtain an infinite sequence of numbers $\alpha, \beta, \gamma, \ldots$ whose norms are all in absolute value $\leq |\sqrt{d}\,|$ and which, in addition, satisfy the conditions $L(\alpha) < L(\beta) < L(\gamma) < \ldots$. Since only finitely many distinct ideals occur as factors of the rational integers with absolute value $\leq |\sqrt{d}\,|$ it follows that in the infinite sequence of principal ideals $(\alpha), (\beta), (\gamma), \ldots$ only finitely many distinct ideals can occur; consequently it happens infinitely often that two of these ideals are equal. If, say, $(\alpha) = (\beta)$ then $\varepsilon = \beta/\alpha$ is a unit and, since $L(\varepsilon) = L(\beta) - L(\alpha) > 0$, ε satisfies the conditions of Lemma 9.

§20. Proof of the Theorem on the Existence of Units

In order to prove Theorem 47 we choose, according to Lemma 9, a unit η_1 in k for which $l_1(\eta_1) \neq 0$, then a unit η_2 for which the determinant

$$\begin{vmatrix} l_1(\eta_1) & l_1(\eta_2) \\ l_2(\eta_1) & l_2(\eta_2) \end{vmatrix} \neq 0;$$

then again we choose a unit η_3 such that

$$\begin{vmatrix} l_1(\eta_1) & l_1(\eta_2) & l_1(\eta_3) \\ l_2(\eta_1) & l_2(\eta_2) & l_2(\eta_3) \\ l_3(\eta_1) & l_3(\eta_2) & l_3(\eta_3) \end{vmatrix} \neq 0$$

and so on in this way until eventually we have a set of units $\eta_1, \ldots, \eta_r$ for which the determinant

$$\begin{vmatrix} l_1(\eta_1) & \cdots & l_1(\eta_r) \\ & \cdots\cdots & \\ l_r(\eta_1) & \cdots & l_r(\eta_r) \end{vmatrix} \neq 0.$$

It follows from this that if H is any unit of the field the first r logarithms of H can be put in the form

$$\begin{aligned} l_1(\mathsf{H}) &= e_1 l_1(\eta_1) + \cdots + e_r l_1(\eta_r), \\ &\cdots\cdots\cdots \\ l_r(\mathsf{H}) &= e_1 l_r(\eta_1) + \cdots + e_r l_r(\eta_r), \end{aligned}$$

where $e_1, \ldots, e_r$ are real numbers. This representation shows that we may write

$$\begin{aligned} l_1(\mathsf{H}) &= m_1 l_1(\eta_1) + \cdots + m_r l_1(\eta_r) + E_1, \\ &\cdots\cdots\cdots \\ l_r(\mathsf{H}) &= m_1 l_r(\eta_1) + \cdots + m_r l_r(\eta_r) + E_r, \end{aligned}$$

where $m_1, \ldots, m_r$ are the greatest rational integers less than or equal to $e_1, \ldots, e_r$ respectively and the numbers $E_1, \ldots, E_r$ have the form

$$\begin{aligned} E_1 &= \mu_1 l_1(\eta_1) + \cdots + \mu_r l_1(\eta_r), \\ &\cdots\cdots\cdots \\ E_r &= \mu_1 l_r(\eta_1) + \cdots + \mu_r l_r(\eta_r), \end{aligned}$$

where $\mu_1, \ldots, \mu_r$ are real numbers ≥ 0 and < 1. Thus $E_1, \ldots, E_r$ are bounded in absolute value by a bound κ which is independent of H. So the first r logarithms of the unit

$$\overline{\mathsf{H}} = \frac{\mathsf{H}}{\eta_1^{m_1} \cdots \eta_r^{m_r}}$$

are all bounded in absolute value by κ. Since $l_1(\overline{\mathsf{H}})+\ldots+l_{r+1}(\overline{\mathsf{H}}) = 0$ it follows that $l_{r+1}(\overline{\mathsf{H}})$ is in absolute value less than $r\kappa$. Thus we have the inequalities

$$|\overline{\mathsf{H}}^{(1)}| < e^{\kappa}, \ldots, |\overline{\mathsf{H}}^{(r)}| < e^{\kappa}, |\overline{\mathsf{H}}^{(r+1)}| < e^{r\kappa},$$

and so all the conjugate values of the unit $\overline{\mathsf{H}}$ are less in absolute value than $e^{r\kappa}$.

According to Theorem 43 there can be only finitely many such units. Let us denote them by $\mathsf{H}_1, \ldots, \mathsf{H}_G$. It follows that $\overline{\mathsf{H}} = \mathsf{H}_S$ or $\mathsf{H} = \mathsf{H}_S \eta_1^{m_1} \ldots \eta_r^{m_r}$ where S is one of the numbers 1, 2, $\ldots G$. If H_T is one of the G units $\mathsf{H}_1, \ldots, \mathsf{H}_G$ and we form the first $G+1$ powers of H_T, then, by what we have just proved, some two of these powers must be expressible in the forms $\mathsf{H}_S \eta_1^{m_1'} \cdots \eta_r^{m_r'}$ and $\mathsf{H}_S \eta_1^{m_1''} \cdots \eta_r^{m_r''}$ (with the same H_S in both cases); hence their quotient can be represented in the form $\eta_1^{m_1} \cdots \eta_r^{m_r}$. So we have proved that for each unit H_T there is an exponent M_T such that $\mathsf{H}_T^{M_T}$ is a product of powers of the units $\eta_1, \ldots, \eta_r$. Let M be the least common multiple of the G exponents $M_1, \ldots, M_G$, so that the exponent M has the same property for all G units $\mathsf{H}_1, \ldots, \mathsf{H}_G$. From this it follows that the first r logarithms of each unit H of the field k have the form

$$\left.\begin{aligned} l_1(\mathsf{H}) &= \frac{m_1 l_1(\eta_1) + \cdots + m_r l_1(\eta_r)}{M} \\ &\cdots\cdots\cdots \\ l_r(\mathsf{H}) &= \frac{m_1 l_r(\eta_1) + \cdots + m_r l_r(\eta_r)}{M} \end{aligned}\right\} \tag{6.5}$$

where $m_1, \ldots, m_r$ are rational integers.

We now apply to the infinite set (6.5) of logarithms of all units the same line of argument as we used in Theorem 5 (Sect. 3) to prove the existence of a field basis. It follows that there is a set of r units $\varepsilon_1, \ldots, \varepsilon_r$ by means of whose logarithms the logarithms of each arbitrary unit H can be expressed in the form

$$\begin{aligned} l_1(\mathsf{H}) &= a_1 l_1(\varepsilon_1) + \cdots + a_r l_1(\varepsilon_r), \\ &\cdots\cdots\cdots \\ l_r(\mathsf{H}) &= a_1 l_r(\varepsilon_1) + \cdots + a_r l_r(\varepsilon_r) \end{aligned}$$

where $a_1, \ldots, a_r$ are rational integers.

We claim that this set of units satisfies the conditions of Theorem 47.

To see this, let H be any unit, whose logarithms have the above form. Then

$$\rho = \frac{\mathsf{H}}{\varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}}$$

is a unit whose logarithms are all zero. Such a unit is necessarily a root of unity. For, according to what we proved earlier, $\rho^M = \eta_1^{m_1} \cdots \eta_r^{m_r}$, where $m_1, \ldots, m_r$ are rational integers. Taking logarithms we have

$$\begin{aligned} m_1 l_1(\eta_1) + \cdots + m_r l_1(\eta_r) &= 0, \\ \cdots\cdots\cdots \\ m_1 l_r(\eta_1) + \cdots + m_r l_r(\eta_r) &= 0, \end{aligned}$$

whence $m_1 = m_2 = \ldots = m_r = 0$ and $\rho^M = 1$. This gives a representation of the unit H as described in Theorem 47.

From the method used to determine the units $\varepsilon_1, \ldots, \varepsilon_r$ it follows that

$$\begin{vmatrix} l_1(\eta_1) & \cdots & l_1(\eta_r) \\ & \cdots\cdots & \\ l_r(\eta_1) & \cdots & l_r(\eta_r) \end{vmatrix} = AR$$

where A is a rational integer and R is an abbreviation for

$$\begin{vmatrix} l_1(\varepsilon_1) & \cdots & l_1(\varepsilon_r) \\ & \cdots\cdots & \\ l_r(\varepsilon_1) & \cdots & l_r(\varepsilon_r) \end{vmatrix}.$$

This determinant R is nonzero and from this it follows that the representation of the unit H by means of the units $\varepsilon_1, \ldots, \varepsilon_r$ is unique. We have thus succeeded in proving all the assertions of the fundamental Theorem 47.

§21. Fundamental Sets of Units. Regulator of a Field. Independent Sets of Units

A set of units $\varepsilon_1, \ldots, \varepsilon_r$ with the property set out in Theorem 47 is called a *fundamental set of units* of the field k. It follows easily that when $\varepsilon_1^*, \ldots, \varepsilon_r^*$ is another fundamental set of units the determinant of the first r logarithms of these r units coincides with R up to sign. We always choose the order of a fundamental set of units so that R is a positive number. The number R is then uniquely determined by the field k; we call R the *regulator* of the field k.

We showed in the proof of Theorem 47 that a unit all of whose logarithms are zero must be a root of unity. This fact is expressed also in the following theorem, which can actually be easily established directly (*Kronecker* (6), *Minkowski* (3)).

Theorem 48. *A unit which, together with all its conjugates, has absolute value* 1 *is a root of unity.*

Since the two roots of unity $+1$ and -1 occur in every field the number of roots of unity in a field k is always even; clearly this number can exceed 2 only if all m conjugate fields are imaginary.

An arbitrary set of t units, $\eta_1, \ldots, \eta_t$ is called an *independent set* if there exists no relation of the form $\eta_1^{m_1} \cdots \eta_t^{m_t} = 1$ where $m_1, \ldots, m_t$ are rational integers not all zero. The number t cannot exceed r; in particular a fundamental set $\varepsilon_1, \ldots, \varepsilon_r$ is an independent set of r units. On the other hand, if we have an independent set of r units $\eta_1, \ldots, \eta_r$ there exists a rational integer M such that for every unit ε of the field k there is an equation of the form $\varepsilon^M = \eta_1^{m_1} \cdots \eta_r^{m_r}$ where $m_1, \ldots, m_r$ are rational integers. For if $\eta_s = \rho_s \varepsilon_1^{a_{1s}} \cdots \varepsilon_r^{a_{rs}}$ for $s = 1, \ldots, r$, where ρ_s is a root of unity and a_{1s}, $\ldots, a_{rs}$ are integer exponents, then (by the hypothesis that $\eta_1, \ldots, \eta_r$ form an independent set) the determinant of the exponents $a_{11}, \ldots, a_{rr}$ must be nonzero. If this determinant is denoted by A it follows that the A-th power of each unit ε of the field is equal to a product of powers of the units $\eta_1, \ldots,$ η_r multiplied by a root of unity ρ. If $\rho^E = 1$ for all roots of unity ρ in k then obviously the exponent $M = AE$ has the desired property.

The above proof of Theorem 47 also shows that it is possible to determine a fundamental set of units by means of a finite number of rational operations. A more detailed investigation of the problem of finding the simplest way to calculate the units leads to the theory of continued fraction algorithms, where the wider question of the periodicity of such developments is of particular interest (*Minkowski* (3,4)).

7. Ideal Classes of a Field

§22. Ideal Classes. Finiteness of the Class Number

Every integer of a number field k determines a principal ideal; every *fraction*, i.e. every number κ of k which is not an integer, can be represented as the quotient of two integers α and β and hence as the quotient of two ideals $\mathfrak{a}$ and $\mathfrak{b}$: $\kappa = \alpha/\beta = \mathfrak{a}/\mathfrak{b}$. If we require that the ideals $\mathfrak{a}$ and $\mathfrak{b}$ have no common ideal factor then the representation of the fraction κ as a quotient of ideals is uniquely determined. Conversely, if the quotient $\mathfrak{a}/\mathfrak{b}$ of two ideals $\mathfrak{a}$ and $\mathfrak{b}$ – with or without a common factor – is equal to an integer or a fraction $\kappa = \alpha/\beta$ of the field, we say that the two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are *equivalent* to one another, denoted by $\mathfrak{a} \sim \mathfrak{b}$. If $\mathfrak{a}/\mathfrak{b} = \alpha/\beta$ then we have $(\beta)\mathfrak{a} = (\alpha)\mathfrak{b}$ and so we recognise that two ideals are equivalent to one another if and only if they are transformed into the same ideal when they are multiplied by suitable principal ideals. The totality of all ideals which are equivalent to a given ideal is called an *ideal class*. All principal ideals are equivalent to the principal ideal (1); the class which they form is called the *principal class* and is denoted by 1. If $\mathfrak{a} \sim \mathfrak{a}'$ and $\mathfrak{b} \sim \mathfrak{b}'$ then we have $\mathfrak{a}\mathfrak{b} \sim \mathfrak{a}'\mathfrak{b}'$. If A is the ideal class containing the ideal $\mathfrak{a}$ and B is the ideal class containing $\mathfrak{b}$ then the ideal class containing $\mathfrak{a}\mathfrak{b}$ is called the *product of the ideal classes* A and B and is denoted by AB. Obviously $1B = B$ and conversely from $AB = B$ it follows that $A = 1$.

It is sometimes useful to work with ideal quotients: an equation of the form $\mathfrak{a}/\mathfrak{a}' = \mathfrak{b}/\mathfrak{b}'$ or an equivalence of the form $\mathfrak{a}/\mathfrak{a}' \sim \mathfrak{b}/\mathfrak{b}'$ are to be taken as synonymous with the equation or equivalence produced on multiplying by the ideals in the denominators, i.e. with the equation $\mathfrak{a}\mathfrak{b}' = \mathfrak{a}'\mathfrak{b}$ or the equivalence $\mathfrak{a}\mathfrak{b}' \sim \mathfrak{a}'\mathfrak{b}$ respectively.

We have the following theorem.

Theorem 49. *Let A be an ideal class; then there exists one and only one ideal class B whose product with A is is the principal class.*

Proof. Let $\mathfrak{a}$ be an ideal in the class A and α an integer divisible by $\mathfrak{a}$, so that we may write $\alpha = \mathfrak{a}\mathfrak{b}$. Then if B is the class of the ideal $\mathfrak{b}$ we have

$AB = 1$. If there were another class B' such that $AB' = 1$ then, on multiplication by B, we have $B = ABB' = B'$.

The class B' is called the *inverse class* of A and is denoted by A^{-1}. We have also the following fundamental result.

Theorem 50. *In every ideal class there exists an ideal whose norm does not exceed the absolute value of the square root of the discriminant of the field (Minkowski (1, 3)). The number of ideal classes of a number field is finite (Dedekind (1), Kronecker (16)).*

Proof. Let A be an ideal class and $\mathfrak{i}$ an ideal in the inverse class A^{-1}. Then, according to Theorem 46, there is an integer ι divisible by $\mathfrak{i}$ whose norm satisfies the condition $|n(\iota)| \leq n(\mathfrak{i})|\sqrt{d}\,|$. If we set $\iota = \mathfrak{i}\mathfrak{a}$ then $\mathfrak{a}$ belongs to the ideal class A and since $|n(\iota)| = n(\mathfrak{i})n(\mathfrak{a})$ it follows that $n(\mathfrak{a}) \leq |\sqrt{d}\,|$. Thus there exists in the class A an ideal $\mathfrak{a}$ satisfying the latter condition.

Since the rational integers which are $\leq |\sqrt{d}\,|$ have only finitely many distinct ideals as factors, the second assertion of the theorem follows at once.

The number of ideal classes of a field k is called the *class number* of k.

§23. Applications of the Theorem on the Finiteness of the Class Number

Theorem 50 which we have just proved has many consequences and applications, of which we emphasize the following.

Theorem 51. *If h is the number of ideal classes then the h-th power of each class is the principal class.*

Proof. In the sequence $A, A^2, \ldots, A^{h+1}$ there must be two classes which coincide, say $A^r = A^{r+e}$. Since $A^rA^e = A^r$ we have $A^e = 1$. Let e be the smallest positive exponent such that $A^e = 1$; then the e classes $A^0 = 1, A, \ldots, A^{e-1}$ are all distinct. If B is a class distinct from these e classes then the e classes $B, AB, \ldots, A^{e-1}B$ are again all distinct from one another and from all the previous e classes. Continuing in this way we see that h must be a multiple of e and from this the result of the Theorem follows.

According to Theorem 51 the h-th power of every ideal $\mathfrak{a}$ is a principal ideal.

Theorem 52. *If α and β are arbitrary integers there exists a nonzero integer γ dividing both α and β which can be expressed in the form*

$\gamma = \xi\alpha + \eta\beta$, where ξ and η are suitably chosen integers. In general γ, ξ and η do not belong to the number field determined by α and β (Dedekind (1)).

Theorem 53. *Let κ, ρ and κ^*, ρ^* be two pairs of numbers in the field k. In order that $\mathfrak{i} = (\kappa, \rho) = (\kappa^*, \rho^*)$ it is necessary and sufficient that there be four integers α, β, γ, δ in k whose determinant $\alpha\delta - \beta\gamma = 1$ and which satisfy the equations*

$$\begin{aligned} \kappa^* &= \alpha\kappa + \beta\rho, \\ \rho^* &= \gamma\kappa + \delta\rho \end{aligned}$$

(*Hurwitz* (4)).

Proof. That the condition is sufficient follows from the fact that these two equations have a solution of the form

$$\begin{aligned} \kappa &= \alpha^*\kappa^* + \beta^*\rho^*, \\ \rho &= \gamma^*\kappa^* + \delta^*\rho^* \end{aligned}$$

where α^*, β^*, γ^*, δ^* are integers.

To see that the condition is also necessary, let h be the number of ideal classes. Then $\mathfrak{i}^h = (\kappa^h, \rho^h) = ((\kappa^*)^h, (\rho^*)^h) = (\tau)$, where τ is an integer of the field k. Let

$$\tau = \mu\kappa^h + \nu\rho^h = \mu^*(\kappa^*)^h + \nu^*(\rho^*)^h$$

where μ, ν, μ^*, ν^* are integers in k. Then it is clear that the four integers

$$\begin{aligned} \alpha &= \frac{\mu\kappa^*\kappa^{h-1} + \nu^*\rho(\rho^*)^{h-1}}{\tau} \\ \beta &= \frac{\nu\kappa^*\rho^{h-1} - \nu^*\kappa(\rho^*)^{h-1}}{\tau} \\ \gamma &= \frac{\mu\rho^*\kappa^{h-1} - \mu^*\rho(\kappa^*)^{h-1}}{\tau} \\ \delta &= \frac{\nu\rho^*\rho^{h-1} + \mu^*\kappa(\kappa^*)^{h-1}}{\tau} \end{aligned}$$

satisfy the conditions of Theorem 53. That $\alpha\delta - \beta\gamma = 1$ follows when we combine the determinants

$$-\tau = \begin{vmatrix} \mu\kappa^{h-1} & \rho \\ \nu\rho^{h-1} & -\kappa \end{vmatrix} \quad \text{and} \quad -\tau = \begin{vmatrix} \kappa^* & \nu^*(\rho^*)^{h-1} \\ \rho^* & -\mu^*(\kappa^*)^{h-1} \end{vmatrix}$$

using the multiplication theorem.

According to Theorem 12 each ideal of k can be represented in the form $\mathfrak{i} = (\kappa, \rho)$. If we set $\vartheta = \kappa/\rho$ then the integral or fractional number ϑ determines completely the ideal class to which $\mathfrak{i}$ belongs. We call ϑ the *numerical*

fraction associated with the ideal class. Theorem 53 shows that if $\vartheta^* = \kappa^*/\rho^*$ is another numerical fraction associated with the same ideal class then there must exist four integers α, β, γ, δ in k with determinant 1 such that

$$\vartheta^* = \frac{\alpha\vartheta + \beta}{\gamma\vartheta + \delta}.$$

§24. The Set of Ideal Classes. Strict Form of the Class Concept

The proof of Theorem 50 gives us at the same time a simple method for constructing, by means of a finite number of rational processes, a complete set of inequivalent ideals for each given field. We need to take into consideration only those ideals whose norm $\leq |\sqrt{d}|$. In order to determine completely any equivalence which occurs between these ideals we need only multiply all of them in pairs and in each resulting product $\mathfrak{i}$ search for a nonzero number ι whose norm is smallest in absolute value, in order to see whether $\mathfrak{i} = (\iota)$, in which case the factors of the product belong to inverse classes. It follows from Theorem 46 that this also requires only a finite number of operations. Namely, if $\iota_1, \ldots, \iota_m$ is a basis for the ideal $\mathfrak{i}$ we have only to determine rational integers $u_1, \ldots, u_m$, not all zero, such that the absolute values of the real and imaginary parts of $u_1\iota_1^{(s)} + \cdots + u_m\iota_m^{(s)}$ for $s = 1, \ldots, m$ are all less than certain given bounds. This requires only a finite number of tests. In the same way also we see that to determine for each given ideal the ideal class to which it belongs requires only a finite number of rational operations.

We notice that in certain circumstances a stricter form of the equivalence and class concepts is useful, in which two ideals are said to be *strictly equivalent* only if their quotient is an integer or fraction with positive norm (*Dedekind* (1)).

§25. A Lemma on the Asymptotic Value of the Number of All Principal Ideals Divisible by a Given Ideal

Following the example of Dirichlet who expressed the number of classes of binary quadratic forms with given determinant by transcendental methods (*Dirichlet* (7,8)) and on the basis of the results contained in Chapter 6 on the units of a number field, Dedekind succeeded in deducing a fundamental formula representing the number h of ideal classes of an arbitrary number field as the sum of a certain infinite series (*Dedekind* (1)). In order to derive this formula we prove first the following lemma.

Lemma 10. *Let $\mathfrak{a}$ be an ideal of k; let t be a positive real variable and T the number of all principal ideals which are divisible by $\mathfrak{a}$ and whose norms are $\leq t$. Then*

$$\lim_{t\to\infty} \frac{T}{t} = \frac{2^{r_1+r_2}\pi^{r_2}}{w} \frac{1}{n(\mathfrak{a})} \frac{R}{|\sqrt{d}\,|},$$

where w is the number of roots of unity in k, R is the regulator of k and r_1, r_2 are as explained in Theorem 47.

Proof. Let $\alpha_1, \ldots, \alpha_m$ be a basis of the ideal $\mathfrak{a}$; then every integer divisible by $\mathfrak{a}$ has the form

$$\eta = \eta(v) = v_1\alpha_1 + \cdots + v_m\alpha_m = f_1(v)\omega_1 + \cdots + f_m(v)\omega_m,$$

where $v_1, \ldots, v_m$ take rational integer values and $f_1(v), \ldots, f_m(v)$ are linear functions of $v_1, \ldots, v_m$ with integer coefficients. If we consider $v_1, \ldots, v_m$ as real variables and set

$$u_1 = \frac{f_1(v)}{|\sqrt[m]{n(\eta)}|}, \ldots, u_m = \frac{f_m(v)}{|\sqrt[m]{n(\eta)}|},$$

$$\xi = \xi(v) = u_1\omega_1 + \cdots + u_m\omega_m = \frac{\eta(v)}{|\sqrt[m]{n(\eta)}|}$$

then $u_1, \ldots, u_m$ are one-valued functions of $v_1, \ldots, v_m$ and ξ is a form for which $n(\xi) = \pm 1$. We calculate now the first r logarithms of the form ξ and then r real numbers $e_1(\xi), \ldots, e_r(\xi)$ such that if $\varepsilon_1, \ldots, \varepsilon_r$ form a fundamental set of units we have

$$\begin{aligned} l_1(\xi) &= e_1(\xi)l_1(\varepsilon_1) + \cdots + e_r(\xi)l_1(\varepsilon_r) \\ &\cdots\cdots\cdots \\ l_r(\xi) &= e_1(\xi)l_r(\varepsilon_1) + \cdots + e_r(\xi)l_r(\varepsilon_r). \end{aligned}$$

In this Section 25 we shall refer to these numbers $e_1, \ldots, e_r$ as the r *exponents* of η.

If we take $v_1, \ldots, v_m$ to be rational integers, not all zero, it is clear that the integer η so formed can always be transformed by multiplying by integral powers of the units $\varepsilon_1, \ldots, \varepsilon_r$ into a number whose exponents $e_1, \ldots, e_r$ satisfy the conditions

$$0 \leq e_1 < 1, \ldots, 0 \leq e_r < 1. \tag{7.1}$$

Conversely we see that two integers η, η^*, whose norms and exponents are equal can differ from one another only by a factor which is a root of unity. Thus, if w is the number of roots of unity lying in k, then the product of w and T, the number of all principal ideals divisible by $\mathfrak{a}$ with norm $\leq t$, must be equal to the number of different sets of integers $v_1, \ldots, v_m$ for which

$|n(\eta)| \leq t$ and for which in addition the exponents $e_1, \ldots, e_r$ satisfy the conditions (7.1).

Now we set

$$\tau = t^{-1/m}, v_1 = \varphi_1/\tau, \ldots, v_m = \varphi_m/\tau;$$

then the form ξ, and consequently also the numbers $l_1(\xi), \ldots, l_r(\xi)$ and $e_1, \ldots, e_r$ become independent of τ and involve only the m new variables $\varphi_1, \ldots, \varphi_m$. The inequality $|n(\eta)| \leq t$ becomes $|n(\eta(\varphi))| \leq 1$; furthermore, as a consequence of the conditions (7.1), the r logarithms $l_1(\xi), \ldots, l_r(\xi)$ (and hence also, since $l_1(\xi) + \cdots + l_{r+1}(\xi) = ln(\xi) = 0$, the logarithm $l_{r+1}(\xi)$) are in absolute value less than a finite bound which depends on $\varepsilon_1, \ldots, \varepsilon_r$. The same holds for all the numbers $|\xi^{(1)}(\varphi)|, \ldots, |\xi^{(m)}(\varphi)|$ and hence also, since $|n(\eta(\varphi))| \leq 1$, all the m numbers $|\eta^{(1)}(\varphi)|, \ldots, |\eta^{(m)}(\varphi)|$ are less than a fixed bound. From this it follows that the inequalities (7.1) together with the inequality $|n(\eta(\varphi))| \leq 1$ bound a finite domain in the m-dimensional space of the coordinates $\varphi_1, \ldots, \varphi_m$.

Now we bear in mind that according to a remark in Sect. 19 (p. 46) the function values $l_1(\eta), \ldots, l_m(\eta)$ determine the values $\varphi_1, \ldots, \varphi_m$ in a 2^{r_1}-valued way. Hence

$$\lim_{\tau \to 0} \{wT\tau^m\} = 2^{r_1} \int \cdots \int d\varphi_1 d\varphi_2 \ldots d\varphi_m$$

where the integral on the right hand side is taken over the m-dimensional domain determined by the inequalities

$$0 \leq e_1 \leq 1, \ \ldots, \ 0 \leq e_r \leq 1, \ |n(\eta(\varphi))| \leq 1$$

and hence has a determinate finite value.

To find this value we introduce new variables of integration in place of $\varphi_1, \ldots, \varphi_m$; namely we set

$$\psi_1 = e_1(\xi), \ldots, \psi_r = e_r(\xi), \psi_{r+1} = |n(\eta)|, \psi_{r+2} = l_{r+2}(\xi), \ldots, \psi_m = l_m(\xi)$$

where ξ and η depend on $\varphi_1, \ldots, \varphi_m$. Since these m quantities are all analytic and regular one-valued functions of $\varphi_1, \ldots, \varphi_m$ in the domain

$$0 \leq \psi_1 \leq 1, \ldots, 0 \leq \psi_r \leq 1, 0 \leq \psi_{r+1} \leq 1,$$

$$0 \leq \psi_{r+2} \leq 2\pi, \ldots, 0 \leq \psi_m \leq 2\pi,$$

we have

$$\int \cdots \int d\varphi_1 \ldots d\varphi_m = \int \cdots \int \left| \frac{\varphi_1, \ldots, \varphi_m}{\psi_1, \ldots, \psi_m} \right| d\psi_1 \ldots d\psi_m.$$

According to what was said in Sect. 19 (p. 46) we have

$$\left|\frac{f_1,\ldots,f_m}{l_1(\eta),\ldots,l_m(\eta)}\right| = \left|\frac{n(\eta)}{\sqrt{d}}\right|.$$

Furthermore, since

$$ln(\eta) = l_1(\eta) + \cdots + l_{r+1}(\eta)$$

and

$$l_s(\xi) = l_s(\eta) - \frac{1}{m}ln(\eta) \qquad (s = 1, 2, \ldots, r),$$

we have the following relations

$$\left|\frac{l_1(\eta),\ldots,l_r(\eta),l_{r+1}(\eta)}{l_1(\eta),\ldots,l_r(\eta),ln(\eta)}\right| = 1, \quad \left|\frac{l_1(\eta),\ldots,l_r(\eta),ln(\eta)}{l_1(\xi),\ldots,l_r(\xi),ln(\eta)}\right| = 1$$

and, since finally

$$l_{r+2}(\eta) = l_{r+2}(\xi), \ldots, l_m(\eta) = l_m(\xi),$$

$$\left|\frac{ln(\eta)}{n(\eta)}\right| = \frac{1}{|n(\eta)|}, \quad \left|\frac{\varphi_1,\ldots,\varphi_m}{f_1(\varphi),\ldots,f_m(\varphi)}\right| = \frac{1}{n(\mathfrak{a})}, \quad \left|\frac{l_1(\xi),\ldots,l_r(\xi)}{\psi_1,\ldots,\psi_r}\right| = R,$$

we obtain by multiplying all these equations

$$\left|\frac{\varphi_1,\ldots,\varphi_m}{\psi_1,\ldots,\psi_m}\right| = \frac{R}{n(\mathfrak{a})|\sqrt{d}|}.$$

Hence the above integral has the value

$$\frac{(2\pi)^{r_2}R}{n(\mathfrak{a})|\sqrt{d}|};$$

this completes the proof of Lemma 10.

In the sequel we shall write

$$\kappa = \frac{2^{r_1+r_2}\pi^{r_2}}{w}\,\frac{R}{|\sqrt{d}|}$$

so that κ is a number determined by the field alone and a characteristic number for it.

§26. Determination of the Class Number by the Residue of the Function $\zeta(s)$ at $s = 1$

Theorem 54. *If T is the number of ideals in a class A with norm $\leq t$ then we have*

$$\lim_{t\to\infty} T/t = \kappa.$$

Proof. Let $\mathfrak{a}$ be an ideal of the inverse class A^{-1} of A and let $\mathfrak{r}$ run through all the ideals of the class A so that the product $\mathfrak{r}\mathfrak{a}$ represents all the principal ideals divisible by $\mathfrak{a}$ each once only. If in the formula of Lemma 10 we set $t = n(\mathfrak{a})t'$ then T is the number of ideals $\mathfrak{r}$ in A for which $n(\mathfrak{r}) \leq t'$. By cancelling the factor $n(\mathfrak{a})$ we obtain the required formula for $t = t'$.

Since the number κ is independent of the choice of the class A we deduce the following result immediately from Theorem 54.

Theorem 55. *If T is the number of all ideals of the field k with norm $\leq t$ and h is the number of ideal classes then*

$$\lim_{t\to\infty} T/t = h\kappa.$$

From this formula we can deduce by analytic methods a fundamental formula for the class number h. Namely, we have the following.

Theorem 56. *The infinite series*

$$\zeta(s) = \sum_{(\mathfrak{i})} \frac{1}{(n(\mathfrak{i}))^s},$$

in which $\mathfrak{i}$ runs through all ideals of the field, converges for all real numbers $s > 1$ and

$$\lim_{s=1}\{(s-1)\zeta(s)\} = h\kappa$$

(*Dedekind* (1)).

Proof. We denote by $F(n)$ the number of distinct ideals with norm n. Then it is clear that when T has the meaning described in Theorem 55 we have

$$\lim_{t\to\infty} T/t = \lim_{n\to\infty} \frac{F(1) + F(2) + \cdots + F(n)}{n}.$$

The limit on the right hand side can now, as we shall show, be represented as the sum of an infinite series (*Dirichlet* (15)). We arrange all the ideals $\mathfrak{i}$ of the field according to increasing value of their norms, writing the resulting

sequence as $\mathfrak{i}_1, \mathfrak{i}_2, \ldots, \mathfrak{i}_t, \ldots$; we denote the norm of each ideal $\mathfrak{i}_t$ by n_t. Then we have

$$F(1) + \cdots + F(n_t - 1) < t \leq F(1) + \cdots + F(n_t)$$

or

$$\frac{F(1) + \cdots + F(n_t - 1)}{n_t - 1}\left(1 - \frac{1}{n_t}\right) < \frac{t}{n_t} \leq \frac{F(1) + \cdots + F(n_t)}{n_t}.$$

It follows from this according to Theorem 55 that $\lim_{t\to\infty} t/n_t = h\kappa$; that is to say, for every positive real number δ, however small, it is always possible to choose an integer t so large that the inequalities

$$\frac{h\kappa - \delta}{t'} < \frac{1}{n_{t'}} < \frac{h\kappa + \delta}{t'} \tag{7.2}$$

hold for all integers $t' \geq t$.

On the other hand it is well-known that if s is any real number greater than 1 then the series

$$\sum_{(t)} \frac{1}{t^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

converges and that

$$\lim_{s=1}\left\{(s-1)\sum_{(t)} \frac{1}{t^s}\right\} = 1.$$

This last equation shows that we also have

$$\lim_{s=1}\left\{(s-1)\sum_{(t')} \frac{1}{(t')^s}\right\} = 1$$

where t' runs only through the integers which exceed any arbitrarily large bound t. From the convergence of the series $\sum 1/t^s$ we deduce, with the help of the inequality $1/n_t' < (h\kappa + \delta)/t'$, the convergence for $s > 1$ of the series

$$\sum_{(t)} \frac{1}{n_t^s} = \sum_{(\mathfrak{i})} \frac{1}{n(\mathfrak{i})^s}$$

where t runs over all positive integers and $\mathfrak{i}$ runs over all ideals of the field k. Further, it follows from the inequalities (7.2) that

$$(h\kappa - \delta)^s (s-1) \sum_{(t')} \frac{1}{(t')^s} < (s-1) \sum_{(t')} \frac{1}{n_{t'}^s} < (h\kappa + \delta)^s (s-1) \sum_{(t')} \frac{1}{(t')^s}$$

where the sums are taken over all integers t' which are $\geq t$. Taking limits as $s \to 1$ we have that

$$h\kappa - \delta \leq \lim_{s=1}\left\{(s-1)\sum_{(t')} \frac{1}{n_{t'}^s}\right\} \leq h\kappa + \delta.$$

Now we see that

$$\lim_{s=1}\left\{(s-1)\sum_{\mathfrak{i}}\frac{1}{(n(\mathfrak{i}))^s}\right\}=\lim_{s=1}\left\{(s-1)\sum_{(t)}\frac{1}{n_t^s}\right\}=\lim_{s=1}\left\{(s-1)\sum_{(t')}\frac{1}{n_t'^s}\right\}$$

is both $\geq h\kappa-\delta$ and $\leq h\kappa+\delta$; hence, since δ is an arbitrarily small number, the limit is $h\kappa$. This completes the proof of Theorem 56.

§27. Alternative Infinite Expansions of the Function $\zeta(s)$

The function $\zeta(s)$ can be represented in three different ways by infinite expansions (*Dedekind* (1)).

We easily see that

$$\begin{aligned}\zeta(s) &= \sum_{(n)}\frac{F(n)}{n^s}\\ &= \prod_{(\mathfrak{p})}\frac{1}{1-(n(\mathfrak{p}))^{-s}}\\ &= \prod_{(p)}\left(\frac{1}{1-p^{-f_1 s}}\,\frac{1}{1-p^{-f_2 s}}\cdots\frac{1}{1-p^{-f_e s}}\right)\end{aligned}$$

where in the first expression the sum is taken over all positive integers n, in the second expression the product is taken over all prime ideals $\mathfrak{p}$ of the field k and in the third expression the product extends over all rational prime numbers p – here $f_1, \ldots, f_e$ are the degrees of the e prime ideals of k which divide p. All these infinite sums and products for $\zeta(s)$ converge for $s>1$; since the terms are all positive the convergence is independent of the order of the summands or factors.

§28. Composition of Ideal Classes of a Field

We have the following important theorem concerning the multiplicative structure of the set of ideal classes (*Schering* (1), *Kronecker* (11)).

Theorem 57. *There exist q classes $A_1, \ldots, A_q$ such that every class A can be represented in one and only one way in the form*

$$A=A_1^{x_1}\cdots A_q^{x_q}$$

where the exponents $x_1, \ldots, x_q$ run through the ranges from $0,1,2,\ldots,$

to $h_1 - 1, \ldots, h_q - 1$ *respectively; further,* $A_1^{h_1} = 1, \ldots, A_q^{h_q} = 1$ *and* $h_1 \cdots h_q = h$.

Proof. For each class A we determine the smallest positive exponent e_1 such that $A^{e_1} = 1$. Let h_1 be the greatest among all these exponents e_1 and let H_1 be a class with the exponent h_1. Now for each class A we determine the smallest positive exponent e_2 such that A^{e_2} is equal to a power of H_1. The greatest of these exponents is denoted by h_2; let H_2 be a class leading to the exponent h_2. Next we determine for each class A the smallest positive exponent e_3 such that A^{e_3} is equal to a product of powers of H_1 and H_2; let h_3 be the greatest of the exponents e_3 and H_3 a class corresponding to the exponent h_3. We proceed in this way, obtaining a sequence of classes H_1, H_2, $\ldots$, H_q; we see at once that these classes have the property that each class A can be represented in one and only one way in the form $A = H_1^{x_1} \cdots H_q^{x_q}$, where $x_1, \ldots, x_q$ have values as described in the statement of the theorem.

Now let

$$H_s^{h_s} = H_t^{a_t} H_{t-1}^{a_{t-1}} \cdots H_1^{a_1} \tag{7.3}$$

with $a_t \neq 0$ where $t < s$ and $a_t, a_{t-1}, \ldots, a_1$ are certain integral exponents. According to the defining condition we have $H_s^{h_t} = H_{t-1}^{b_{t-1}} \cdots H_1^{b_1}$, where $b_{t-1}, \ldots, b_1$ are integers. h_t must be divisible by h_s, for, if not, there would be a lower power of H_s than the h_s-th expressible as a product of the classes $H_t, H_{t-1}, \ldots, H_1$. If we set $h_t = h_s l_t$ it follows that$H_t^{a_t l_t}$ can be expressed as a product of the classes $H_{t-1}, \ldots, H_1$; it is therefore necessary that $a_t l_t$ be divisible by h_t and so a_t divisible by h_s. Set $a_t = h_s c_s$ and instead of the class H_s choose the class $H_s' = H_s H_t^{-c_s}$. Equation (7.3) now assumes the simpler form

$$(H_s')^{h_s} = H_{t-1}^{a_{t-1}} \cdots H_1^{a_1}.$$

Repetition of this procedure leads eventually to a class A_s in place of H_s for which the desired relation $A_s^{h_s} = 1$ holds.

In addition the above representation of the classes can be so arranged that the numbers $h_1, \ldots, h_q$ are prime numbers or powers of prime numbers. Namely, if g is one of the numbers $h_1, \ldots, h_q$ which is neither a prime nor a power of a prime, let $g = p'p'' \cdots$, where p', p'', $\ldots$ are powers of distinct prime numbers; if B is the class corresponding to g we write $B' = B^{g/p'}$, $B'' = B^{g/p''}$, $\ldots$. Then $B'^{p'} = 1$, $B''^{p''} = 1$, $\ldots$ and when we express $1/g$ as

$$\frac{1}{g} = \frac{a'}{p'} + \frac{a''}{p''} + \cdots$$

it follows that $B = (B')^{a'}(B'')^{a''} \cdots$. Thus B', B'', $\ldots$ can be introduced instead of B. If the classes $A_1, \ldots, A_q$ are chosen in the way just described we say that they form a *fundamental set of ideal classes.*

§29. Characters of Ideal Classes. Generalisation of the Function $\zeta(s)$

Once a fundamental set of ideal classes has been chosen each class A is uniquely determined by the exponents $x_1, \ldots, x_q$ and hence also by the q roots of unity

$$\chi_1(A) = e^{2\pi i x_1/h_1}, \ldots, \chi_q(A) = e^{2\pi i x_q/h_q}.$$

These q roots of unity $\chi(A)$ are called the *characters of the class* A. If $\chi(A)$, $\chi(B)$ are the characters of the classes A and B respectively we have obviously $\chi(AB) = \chi(A)\chi(B)$. The characters $\chi(A)$ of a class A are also said to be characters $\chi(\mathfrak{a})$ of each ideal $\mathfrak{a}$ contained in the class A.

Using a character χ we can form a function which is a generalisation of the function $\zeta(s)$ considered above and which admits a similar product representation (*Dedekind* (1)). This function is

$$\sum_{(\mathfrak{i})} \frac{\chi(\mathfrak{i})}{(n(\mathfrak{i}))^s} = \prod_{(\mathfrak{p})} \frac{1}{1 - \chi(\mathfrak{p})(n(\mathfrak{p}))^{-s}}$$

where the sum is taken over all ideals $\mathfrak{i}$ and the product over all prime ideals $\mathfrak{p}$ of the field k.

8. Reducible Forms of a Field

§30. Reducible Forms. Form Classes and Their Composition

If $\xi^{(1)}, \ldots, \xi^{(m)}$ are m linear forms in the m variables $u_1, \ldots, u_m$ with arbitrary real or complex coefficients then the product

$$U(u_1,\ldots,u_m) = \xi^{(1)} \cdots \xi^{(m)}$$

is called a *reducible form* of degree m in the m variables $u_1, \ldots, u_m$. The coefficients of the products of $u_1, \ldots, u_m$ are called the *coefficients of the form*. Using the formula

$$-\frac{\partial^2 \log U}{\partial u_r \partial u_s} = \frac{\partial \log \xi^{(1)}}{\partial u_r} \frac{\partial \log \xi^{(1)}}{\partial u_s} + \cdots + \frac{\partial \log \xi^{(m)}}{\partial u_r} \frac{\partial \log \xi^{(m)}}{\partial u_s}$$

$(r, s = 1,\ldots,m)$ we deduce easily by means of the multiplication theorem for determinants that the square of the determinant of the m linear forms $\xi^{(1)}, \ldots, \xi^{(m)}$ is equal to

$$(-1)^m U^2 \sum \pm \frac{\partial^2 \log U}{\partial u_1 \partial u_1} \cdots \frac{\partial^2 \log U}{\partial u_m \partial u_m}$$

and hence is a polynomial with integer coefficients in the coefficients of U; we call this the *discriminant of the form* U. A form whose coefficients are rational integers with no common factor is called a *primitive form*; it is a rational unit form.

Let $\alpha_1, \ldots, \alpha_m$ form a basis for the ideal $\mathfrak{a}$. Then the norm

$$n(\xi) = n(\alpha_1 u_1 + \cdots + \alpha_m u_m)$$

is a reducible form of degree m. The coefficients of $n(\xi)$ are rational integers with highest common factor $n(\mathfrak{a})$. When we cancel this factor we obtain a primitive form U which we call a *reducible form of the field* k. It has the following properties.

If we choose another basis $\alpha_1^*, \ldots, \alpha_m^*$ of the ideal $\mathfrak{a}$ in place of $\alpha_1, \ldots,$ α_m then we obtain a form U^* which is produced from U by means of an integral linear transformation with determinant ± 1. If we call the collection

of all such transforms of a form a *form class* it is clear that to every ideal $\mathfrak{a}$ is associated a definite form class. Obviously the same form class arises when we start with the ideal $\alpha\mathfrak{a}$ instead of $\mathfrak{a}$, where α is any integer or fraction of the field. Thus to every ideal in a given ideal class is associated the same form class.

Since the discriminant of the form $n(\xi) = n(\mathfrak{a})U$ is clearly equal to $n(\mathfrak{a})^2 d$ we have the following result.

Theorem 58. *The discriminant of a reducible form U of a field k is equal to the field discriminant d (Dedekind (1)).*

The properties of the forms U which we have mentioned actually capture their essential nature; namely, the following converse theorem holds.

Theorem 59. *Let U be a primitive form of a field k with degree m and discriminant equal to the field discriminant d. If U is reducible in k but irreducible in every field of lower degree then there exist in k at least one and at most m ideal classes to which the form U is associated.*

Proof. Let $\eta = \mu_1 u_1 + \cdots + \mu_m u_m$ be a linear factor of U with coefficients in k. We multiply η by an integer a so that $\xi = a\eta = \alpha_1 u_1 + \cdots + \alpha_m u_m$ is a linear form with integer coefficients $\alpha_1, \ldots, \alpha_m$. Let $\mathfrak{a} = (\alpha_1, \ldots, \alpha_m)$; then, according to Theorem 20, we have $n(\xi) = n(\mathfrak{a})U$ and since the discriminant of U is equal to the field discriminant it follows that

$$\begin{vmatrix} \alpha_1 & \cdots & \alpha_m \\ \alpha_1' & \cdots & \alpha_m' \\ & \cdots\cdots & \\ \alpha_1^{(m-1)} & \cdots & \alpha_m^{(m-1)} \end{vmatrix}^2 = n(\mathfrak{a})^2 d$$

where $\alpha_1', \ldots, \alpha_i^{(m-1)}$ are the conjugates of α_i $(i = 1, \ldots, m)$. From this equation we deduce, making use of the converse of Theorem 19, that $\alpha_1, \ldots, \alpha_m$ form a basis of the ideal $\mathfrak{a}$.

If the forms U, V are associated to the ideals $\mathfrak{a}$, $\mathfrak{b}$ respectively then every form W associated to the product $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ is called a *composed form* of U and V (*Dedekind* (1)).

According to the above discussion the question whether two given forms of a field k belong to the same form class is equivalent to the question whether two given ideals are equivalent; hence the matter can be decided by means of a finite number of operations (see Sect. 24).

9. Orders in a Field

§31. Orders. Order Ideals and Their Most Important Properties

Let ϑ, η, ... be any algebraic integers whose domain of rationality is the field k[1] of degree m; then the set of all polynomials in ϑ, η, ... with rational integer coefficients is called an *order*[2]. Addition, subtraction and multiplication of two numbers in an order produce again numbers in the order. An order is thus invariant under the three operations of addition, subtraction and multiplication. The maximal order in a field k is the order determined by $\omega_1, \ldots, \omega_m$ where these are numbers of a basis for k; this consists of all the algebraic integers of k. Each order r contains m integers $\rho_1, \ldots, \rho_m$ such that every number ρ of the order can be expressed in the form

$$\rho = a_1\rho_1 + \cdots + a_m\rho_m$$

where $a_1, \ldots, a_m$ are rational integers. The numbers $\rho_1, \ldots, \rho_m$ are called a *basis of the order*. If we denote the conjugates of $\rho_1, \ldots, \rho_m$ by $\rho'_1, \ldots, \rho'_m$, $\ldots, \rho_1^{(m-1)}, \ldots, \rho_m^{(m-1)}$ then the square of the determinant

$$\begin{vmatrix} \rho_1 & \cdots & \rho_m \\ \rho'_1 & \cdots & \rho'_m \\ & \cdots\cdots & \\ \rho_1^{(m-1)} & \cdots & \rho_m^{(m-1)} \end{vmatrix}$$

is a rational number; it is called the *discriminant of the order* r and is denoted by d_r.

An *order ideal* or an *ideal of the order* r is an infinite set $\mathfrak{i}_r$ of algebraic integers $\alpha_1, \alpha_2, \ldots$ in the order r having the property that every linear combination $\lambda_1\alpha_1 + \lambda_2\alpha_2 + \cdots$ of $\alpha_1, \alpha_2, \ldots$ with coefficients $\lambda_1, \lambda_2, \ldots$ drawn from the order r again belongs to $\mathfrak{i}_r$. Every order ideal contains m integers $\iota_1, \ldots, \iota_m$ such that every number in the ideal can be expressed as a linear combination $a_1\iota_1 + \cdots + a_m\iota_m$ where $a_1, \ldots, a_m$ are rational integers. The

[1] i.e. k is the smallest field containing ϑ, η, ...

[2] Hilbert calls it a *number ring* (*Zahlring*), *ring* (*Ring*) or *integral domain* (*Integritätsbereich*) and refers in a footnote to Dedekind's term *Ordnung*.

numbers $\iota_1, \ldots, \iota_m$ are said to be a *basis of the order ideal.* The proofs for the existence of bases for an order and for an order ideal correspond precisely to those in Sect. 3 and 4 for the existence of bases for a field and an ideal. We have the following theorems (*Dedekind* (3)).

Theorem 60. *Let $\iota_1, \ldots, \iota_m$ be any m integers of the field k which satisfy no linear relation with rational integer coefficients. Then there exists an order r in which, for a suitably chosen integer A, the products $A\iota_1, A\iota_2, \ldots, A\iota_m$ form the basis of an order ideal.*

(Compare the proof of this Theorem 60 with that of Theorem 61.)

Proof. Let ρ be an integer of the field for which the m numbers $\rho\iota_1, \ldots, \rho\iota_m$ are all equal to linear combinations of $\iota_1, \ldots, \iota_m$ of the form $a_1\iota_1 + \cdots + a_m\iota_m$ where $a_1, \ldots, a_m$ are rational integers. Then it is easy to see that the collection of all such integers ρ of k forms an order with the desired property.

If $\mathfrak{i}_r$ is an order ideal in the order r and all the elements of $\mathfrak{i}_r$ can be expressed as linear combinations of the s numbers $\alpha_1, \ldots, \alpha_s$ in r with coefficients from r then we write $\mathfrak{i}_r = [\alpha_1, \ldots, \alpha_s]$. In particular we have $\mathfrak{i}_r = [\iota_1, \ldots, \iota_m]$.

Theorem 61. *In every order r there exist order ideals which are also field ideals.*

Proof. We express $\omega_1, \ldots, \omega_m$ by means of the numbers $\rho_1, \ldots, \rho_m$ of a basis of r in the form

$$\omega_i = \frac{a_{i1}\rho_1 + \cdots + a_{im}\rho_m}{A} \qquad (i = 1, 2, \ldots, m)$$

where $a_{i1}, \ldots, a_{im}$ and A are rational integers. It follows that every integer in k which is divisible by A is a number in the order r and consequently every ideal of the field which is divisible by A is at the same time an order ideal of the order r.

The greatest common divisor of all the field ideals which are also order ideals of the order r is called the *conductor of the order r* (*Dedekind* (3)). We easily deduce the following theorem.

Theorem 62. *Every ideal $\mathfrak{i}$ of the field k which is divisible by the conductor of the order r is also an order ideal of r.*

§32. Order Determined by an Integer. Theorem on the Different of an Integer of a Field

The most important orders of a field are those which are determined by a single integer. Dedekind founded his theory of the discriminants of algebraic number fields on the basis of the properties of these special orders (*Dedekind* (6)). We collect Dedekind's principal results in the following theorem.

Theorem 63. *The greatest common divisor of the differents of all the integers of a field is equal to the different $\mathfrak{d}$ of the field. If δ is the different of an integer ϑ which generates k and $\mathfrak{f}$ is the conductor of the order determined by ϑ then $\delta = \mathfrak{f}\mathfrak{d}$.*

Proof. Let $\omega_1, \ldots, \omega_m$ be a field basis for k and let $\omega_1', \ldots, \omega_m', \ldots, \omega_1^{(m-1)}, \ldots, \omega_m^{(m-1)}$ be the conjugates of these m numbers. We form the m-rowed determinant of the m^2 numbers $\omega_h^{(l)}$:

$$\Omega = \begin{vmatrix} \omega_1 & \cdots & \omega_m \\ \omega_1' & \cdots & \omega_m' \\ & \cdots\cdots\cdots & \\ \omega_1^{(m-1)} & \cdots & \omega_m^{(m-1)} \end{vmatrix}.$$

We denote the $(m-1)$-rowed determinants which are cofactors of $\omega_1, \ldots, \omega_m$ by $\Omega_1, \ldots, \Omega_m$ respectively. The m products $\Omega\Omega_1, \ldots, \Omega\Omega_m$ are then integers of the field k and in fact they form a basis of an ideal of k.

To prove that this is the case we multiply the $m-1$ rows of the determinant Ω_h by

$$u + \omega_i', u + \omega_i'', \ldots, u + \omega_i^{(m-1)}, \tag{9.1}$$

where u is an indeterminate. It is clear that the resulting $(m-1)$-rowed determinant has the form

$$f_1(u)\Omega_1 + f_2(u)\Omega_2 + \cdots + f_m(u)\Omega_m,$$

where $f_1, \ldots, f_m$ are integer polynomials in u. On the other hand the product of the $(m-1)$ linear factors (9.1) has the form

$$u^{m-1} + (\omega_i' + \cdots + \omega_i^{(m-1)})u^{m-2} + \cdots = u^{m-1} + (a - \omega_i)u^{m-2} + \cdots,$$

where a is a rational integer. Equating coefficients of u^{m-2} leads to the result that $\omega_i\Omega_h$ is a linear combination of $\Omega_1, \ldots, \Omega_m$ with rational integer coefficients; with this we have established the desired result that $\Omega\Omega_1, \ldots, \Omega\Omega_m$ form the basis of an ideal.

Let us denote in general the $(m-1)$-rowed determinant which is cofactor of $\omega_h^{(l)}$ in Ω by $\Omega_h^{(l)}$; by a well-known theorem in the theory of determinants the m-rowed determinant $|\Omega_h^{(l)}|$ has the value Ω^{m-1}. It follows that the norm of the ideal $\mathfrak{J} = (\Omega\Omega_1, \ldots, \Omega\Omega_m)$ satisfies the equation

$$dn^2(\mathfrak{J}) = |\Omega\Omega_h^{(l)}|^2 = \Omega^{4m-2}$$

and from this we have $n(\mathfrak{J}) = |d|^{m-1}$. Now obviously the discriminant d of the field is divisible by $\mathfrak{J}$; if we set $d = \mathfrak{J}\mathfrak{i}$ it follows that $n(\mathfrak{i}) = |d|$.

Now let ϑ be any generator of the field k; then we may suppose that the members of a basis for k have the form

$$\begin{aligned}
\omega_1 &= 1\\
\omega_2 &= \frac{a_1 + \vartheta}{f_1}\\
\omega_3 &= \frac{a_2 + a_2'\vartheta + \vartheta^2}{f_2}\\
&\ldots\ldots\ldots\\
\omega_m &= \frac{a_{m-1} + a_{m-1}'\vartheta + \cdots + a_{m-1}^{(m-2)}\vartheta^{m-2} + \vartheta^{m-1}}{f_{m-1}}
\end{aligned}$$

where $a_1, a_2, a_2', \ldots, a_{m-1}^{(m-2)}, f_1, \ldots, f_{m-1}$ are rational integers. We now determine the conductor $\mathfrak{f}$ of the order determined by ϑ and represent the numbers of a basis for $\mathfrak{f}$ in the form

$$\begin{aligned}
\rho_1 &= f_1'\\
\rho_2 &= b_1 + f_2'\vartheta\\
\rho_3 &= b_2 + b_2'\vartheta + f_3'\vartheta^2\\
&\ldots\ldots\ldots\\
\rho_m &= b_{m-1} + b_{m-1}'\vartheta + \cdots + b_{m-1}^{(m-2)}\vartheta^{m-2} + f_m'\vartheta^{m-1}
\end{aligned}$$

where $b_1, b_2, b_2', \ldots, b_{m-1}^{(m-2)}, f_1', f_2', \ldots, f_m'$ are rational integers. It follows from Theorem 62 that $\rho_1\omega_m, \rho_2\omega_{m-1}, \ldots, \rho_m\omega_1$ must be integer polynomials in ϑ, from which we deduce that f_1' must be divisible by f_{m-1}, f_2' by f_{m-2}, $\ldots, f_{m-1}'$ by f_1 and consequently the product $f_1'f_2'\ldots f_{m-1}'$ must be divisible by the product $f = f_1f_2\ldots f_{m-1}$. Since $n(\mathfrak{f}) = f_1f_2\ldots f_{m-1}f_1'f_2'\ldots f_{m-1}'f_m'$ we must have $n(\mathfrak{f}) = f^2g$ where g is a rational integer.

We now set

$$\Theta = \begin{vmatrix} 1 & \vartheta & \cdots & \vartheta^{m-1}\\ 1 & \vartheta' & \cdots & (\vartheta')^{m-1}\\ & & \cdots\cdots & \\ 1 & \vartheta^{(m-1)} & \cdots & (\vartheta^{(m-1)})^{m-1}\end{vmatrix}$$

and

$$\mathsf{H} = \begin{vmatrix} 1 & \vartheta' & \cdots & (\vartheta')^{m-2}\\ & & \cdots\cdots & \\ 1 & \vartheta^{(m-1)} & \cdots & (\vartheta^{(m-1)})^{m-2}\end{vmatrix}.$$

Then for the different δ of the number ϑ we have the relation $(-1)^{m-1}n(\delta) = \Theta/\mathsf{H}$ and, according to p. 5 $(-1)^{m(m-1)/2}n(\delta) = \Theta^2 = f^2d$. Furthermore

$$\sum_{h=1}^{m} u_h \Omega\Omega_h =$$

$$\frac{\Theta}{f^2}\begin{vmatrix} u_1 & f_1 u_2 & \cdots & f_{m-1}u_m \\ 1 & a_1+\vartheta' & \cdots & a_{m-1}+\cdots+(\vartheta')^{m-1} \\ & & \cdots\cdots & \\ 1 & a_1+\vartheta^{(m-1)} & \cdots & a_{m-1}+\cdots+(\vartheta^{(m-1)})^{m-1} \end{vmatrix}, \tag{9.2}$$

where $u_1, \ldots, u_m$ are indeterminates. Here we expand the determinant by the first row, writing the result in the form $u_1\mathsf{H}_1+\cdots+u_m\mathsf{H}_m$. We easily see that the numbers $\mathsf{H}_1/\mathsf{H}, \ldots, \mathsf{H}_m/\mathsf{H}$ are all integers of the field k; equation (9.2) shows that they are derived from the numbers $\Omega\Omega_1, \ldots, \Omega\Omega_m$ when these are multiplied by one and the same factor from k. It follows that the m numbers $\mathsf{H}_1/\mathsf{H}, \ldots, \mathsf{H}_m/\mathsf{H}$ also form a basis for an ideal; we shall call this ideal $\mathfrak{m}$.

The numbers in the ideal $\mathfrak{m}$ are all integer polynomials in ϑ. It follows that $\mathfrak{m}$ is divisible by $\mathfrak{f}$ and we set $\mathfrak{m} = \mathfrak{f}\mathfrak{l}$, where $\mathfrak{l}$ is an ideal in k. Equation (9.2) then shows that

$$\mathfrak{J} = \frac{\Theta\mathsf{H}}{f^2}\,\mathfrak{f}\mathfrak{l} = \frac{d\mathfrak{f}\mathfrak{l}}{\delta};$$

taking norms we have

$$|d|^{m-1} = \frac{|d|^m n(\mathfrak{f})n(\mathfrak{l})}{f^2|d|},$$

i.e. $f^2 = n(\mathfrak{f})n(\mathfrak{l})$. On the other hand we proved earlier that $n(\mathfrak{f}) = f^2 g$. Hence we must have $g = 1$ and $n(\mathfrak{l}) = 1$, so that $\mathfrak{l} = 1$; consequently $n(\mathfrak{f}) = f^2$, $\mathfrak{J}\delta = \mathfrak{f}d$ and $\delta = \mathfrak{f}\mathfrak{i}$.

Now let $\mathfrak{p}$ be any given prime ideal of the field k. We prove first that an integer $\vartheta = \rho$ of k can always be found such that the conductor of the order determined by ρ is not divisible by $\mathfrak{p}$. Let p be the rational prime number divisible by $\mathfrak{p}$ and write $p = \mathfrak{p}^e\mathfrak{a}$ where $\mathfrak{a}$ is an ideal prime to $\mathfrak{p}$. Let ρ be an integer of k so chosen that every integer of k is congruent to some polynomial in k modulo an arbitrary high power of $\mathfrak{p}$. The existence of such a number ρ was established in Theorem 29; furthermore the number ρ can be chosen in such a way that it is congruent to 0 modulo $\mathfrak{a}$ (Theorem 25) and is a generator of k. Now let the discriminant $d(\rho)$ of the number ρ be $p^h a$ where a is a rational integer prime to p. Then every integer ω of the field k can be represented in the form $\omega = F(\rho)/a\rho^h$ where $F(\rho)$ is a polynomial in ρ with integer coefficients. In fact if $\omega \equiv H(\rho)$ modulo $\mathfrak{p}^{eh}$ where $H(\rho)$ is an integer polynomial in ρ and we set $\omega = H(\rho) + \omega^*$ it follows that $\omega^*\rho^h$ is divisible by p^h. We set $\omega^*\rho^h = p^h\alpha$ where α is an integer of k. According to Sect. 3 every integer α of k can be expressed in the form $G(\rho)/d(\rho)$ where $G(\rho)$ is a polynomial in ρ with integer coefficients. It follows that $\omega^* = G(\rho)/a\rho^h$ and hence $\omega = (a\rho^h H(\rho) + G(\rho))/a\rho^h$. The property of the number ρ which we have just established shows that the number $a\rho^h$ belongs to the conductor of

the order determined by ρ. Consequently this conductor is not divisible by $\mathfrak{p}$ and so ρ is a number with the desired property.

This discussion shows that the ideal $\mathfrak{i}$ is precisely the greatest common divisor of the differents of all the integers of k. On the other hand it follows from the definition of the field different $\mathfrak{d}$ that this greatest common divisor must contain $\mathfrak{d}$ as a factor; we set $\mathfrak{i} = \mathfrak{h}\mathfrak{d}$. According to Theorem 13 $n(\mathfrak{d})$ is divisible by the discriminant d; so it follows that $n(\mathfrak{i}) = n(\mathfrak{h})da$ where a is a rational integer. Since $n(\mathfrak{i}) = \pm d$ we deduce that $n(\mathfrak{h}) = 1$, whence $\mathfrak{h} = 1$, $a = \pm 1$ and so finally $\mathfrak{i} = \mathfrak{d}$. Thus Theorem 63 is completely established.

From Theorem 63 we deduce easily Theorems 31 and 37 together with the assertion at the end of Sect. 12 concerning the primes dividing the discriminant of a field. To derive this last result we need only examine the factorisation modulo the prime p under consideration of the left hand side of the equation satisfied by $\vartheta = \rho$ and use this in the same way as we did in Sect. 11 for the left hand side of the fundamental equation.

§33. Regular Order Ideals and Their Divisibility Laws

Let r be an order and $\mathfrak{i}_r = [\alpha_1, \ldots, \alpha_s]$ an order ideal of r. The greatest common divisor of the numbers in $\mathfrak{i}_r$ is a field ideal which we denote by $\mathfrak{i} = (\alpha_1, \ldots, \alpha_s)$ and call the *field ideal associated with the order ideal* $\mathfrak{i}_r$. If it happens in particular that the field ideal $\mathfrak{i}$ is prime to the conductor $\mathfrak{f}$ of the order r we call $\mathfrak{i}_r$ a *regular order ideal*. We have the following theorem.

Theorem 64. *If $\mathfrak{i}$ is a field ideal prime to the conductor $\mathfrak{f}$ of the order r then there exists an order ideal $\mathfrak{i}_r$ in r with which the ideal $\mathfrak{i}$ is associated.*

Proof. Consider the set of all numbers in the order r which are divisible by the given field ideal $\mathfrak{i}$; this set forms an order ideal $\mathfrak{i}_r = [\alpha_1, \ldots, \alpha_s]$ in r. Now choose in the conductor $\mathfrak{f}$ of r an integer φ prime to $\mathfrak{i}$ and in the field ideal $\mathfrak{i}$ a number α prime to φ. Then there are integers ψ and β of the field such that $\varphi\psi + \alpha\beta = 1$. Since $\varphi\psi$ is divisible by $\mathfrak{f}$ and hence is a number in the order r, the number $\alpha\beta$ also lies in r. On the other hand $\alpha\beta$ is divisible by $\mathfrak{i}$; so it follows that $1 - \varphi\psi = \alpha\beta$ is in the order ideal $\mathfrak{i}_r$. The field ideal $\mathfrak{i}^* = (\alpha_1, \ldots, \alpha_s)$ associated with the order ideal $\mathfrak{i}_r$ is thus prime to $\mathfrak{f}$. Since $\mathfrak{i}^*$ is divisible by $\mathfrak{i}$ and furthermore divides the product $\mathfrak{f}\mathfrak{i}$ it follows that $\mathfrak{i} = \mathfrak{i}^*$; so $\mathfrak{i}_r$ is shown to be a regular order ideal with which the field ideal $\mathfrak{i}$ is associated. Thus Theorem 64 is established.

The *product of two order ideals* $\mathfrak{a}_r = [\alpha_1, \ldots, \alpha_s]$ and $\mathfrak{b}_r = [\beta_1, \ldots, \beta_t]$ is defined to be the order ideal

$$\mathfrak{a}_r\mathfrak{b}_r = [\alpha_1\beta_1,\ldots,\alpha_s\beta_1,\ldots,\alpha_1\beta_t,\ldots,\alpha_s\beta_t].$$

The following theorem is immediately clear.

Theorem 65. *The field ideal associated with the product of two regular order ideals is the product of the field ideals associated with the factors.*

By virtue of this theorem the divisibility and decomposition laws for regular order ideals correspond perfectly to those for field ideals prime to $\mathfrak{f}$.

Since in what follows we shall be considering only regular order ideals we shall for the sake of brevity omit the prefix "regular"; so from now on an *order ideal* is to be understood as a *regular* order ideal.

It follows from Theorem 23 that in the field k there are always $\varphi(\mathfrak{f})$ integers prime to $\mathfrak{f}$ and mutually incongruent modulo $\mathfrak{f}$. If one of these integers belongs to the order r then obviously so also do all the numbers which are congruent to it modulo $\mathfrak{f}$. The number of integers in the order r which are prime to $\mathfrak{f}$ and mutually incongruent modulo $\mathfrak{f}$ is a factor of $\varphi(\mathfrak{f})$ which we denote by $\varphi_r(\mathfrak{f})$.

By the *norm* $n(\mathfrak{a}_r)$ *of an order ideal* $\mathfrak{a}_r$ we understand the norm of the field ideal $\mathfrak{a}$ associated with $\mathfrak{a}_r$. This definition leads to the elementary theorems on norms for order ideals.

§34. Units of an Order. Order Ideal Classes

The theorem concerning the existence of fundamental units in a field can also be carried over without difficulty to an order; the theorem for an order follows most easily from the corresponding theorem for the units of a field if we notice that, as a result of Theorem 24, every unit of the field when raised to the $\varphi(\mathfrak{f})$-th power becomes a unit of the order r. The theorem for an order has precisely the same form as Theorem 47 for the field k; the number denoted by r in Theorem 47 we shall here denote by s. Let $\varepsilon_1, \ldots, \varepsilon_s$ be a fundamental set of units for the order r, i.e. a set of s units in r such that every unit in r can be expressed as a product whose factors are drawn from $\varepsilon_1, \ldots, \varepsilon_s$ together with the roots of unity in r. The absolute value of the determinant of the first s logarithms of these s units is called the *regulator* R_r *of the order* r. The number of roots of unity lying in the order r is denoted by w_r (*Dedekind* (3)).

Two order ideals $\mathfrak{a}$ and $\mathfrak{b}$ are said to be *equivalent* to one another if there exist two integers λ and μ such that $\mu\mathfrak{a} = \lambda\mathfrak{b}$. We may also take the notion of equivalence in the strict sense mentioned in Sect. 24 and accordingly make the restriction that μ/λ have positive norm. All the order ideals equivalent to one another form an *order ideal class.* An order ideal (α), where α is an integer prime to $\mathfrak{f}$ with positive norm, is called a *principal order ideal*; the class consisting of all such ideals is called the *principal order ideal class.* Further

definitions and theorems concerning the multiplication of order ideal classes correspond exactly to those in Sect. 22, 28 and 29 for the ideal classes of a field; by an argument similar to that in Sect. 22 we prove the finiteness of the number of order ideal classes. The actual determination of this number can be carried out by two different methods, either in a purely arithmetic way or by the use of analytic means, corresponding to our accounts in Sect. 25 and 26. The result we obtain is the following.

Theorem 66. *Let h and h_r be the numbers of ideal classes in the field k and the order r respectively, both with respect to equivalence in the strict sense. Then*

$$\frac{h_r}{h} = \frac{\varphi(\mathfrak{f})}{\varphi_r(\mathfrak{f})}\,\frac{w_r R}{w R_r}.$$

The ideas of Chapter 8 can also be carried over to orders; so we arrive at the notion of the *reducible form belonging to an order ideal class.*

§35. Lattices and Lattice Classes

Let $\mu_1, \ldots, \mu_m$ be m integers of the field k between which there holds no homogeneous linear relation with rational integer coefficients. Then the set of all numbers in k which can be expressed in the form $a_1\mu_1 + \cdots + a_m\mu_m$ with rational integer coefficients $a_1, \ldots, a_m$ is called a *lattice* in the field k and is denoted by $[\mu_1, \ldots, \mu_m]$. Clearly a lattice is invariant under the operations of addition and subtraction. Examples of lattices are the set of all integers of the field k, all ideals, orders and order ideals. Two lattices $[\mu_1, \ldots, \mu_m]$ and $[\lambda_1, \ldots, \lambda_m]$ are called *equivalent* to one another if there exist two integers μ and λ such that $[\mu\mu_1, \ldots, \mu\mu_m] = [\lambda\lambda_1, \ldots, \lambda\lambda_m]$. All lattices equivalent to one another form a *lattice class.* Dedekind used the concept of lattice as foundation for his investigations into algebraic numbers (*Dedekind* (1, 3, 6, 9)).

The square of the determinant

$$\begin{vmatrix} \mu_1 & \cdots & \mu_m \\ \mu_1' & \cdots & \mu_m' \\ & \cdots\cdots & \\ \mu_1^{(m-1)} & \cdots & \mu_m^{(m-1)} \end{vmatrix}$$

is easily seen to be a rational integer and, moreover, to be divisible by the

square of the norm of the ideal $(\mu_1, \dots, \mu_m)$; we denote the quotient of these two squares by ∂. If we form this quotient for any other lattice equivalent to $[\mu_1, \dots, \mu_m]$ we always obtain the same value ∂. So the rational integer ∂ is a characteristic of the lattice class determined by $[\mu_1, \dots, \mu_m]$; we call it the *discriminant of the lattice class.*

The concepts of *reducible form* and *form class* can be defined for lattices in the same way as was done in Sect. 30 for the field itself (*Dedekind* (3)).

Part II

Galois Number Fields

10. Prime Ideals of a Galois Number Field and its Subfields

§36. Unique Factorisation of the Ideals of a Galois Number Field into Prime Ideals

A number field K which coincides with all its conjugate fields is called a *Galois number field.* If k is an arbitrary number field of degree m and $k', \dots, k^{(m-1)}$ are the fields conjugate to k then a new field K can be composed from all the numbers of the fields $k, k', \dots, k^{(m-1)}$; this field K is then a Galois number field which includes all the fields $k, k', \dots, k^{(m-1)}$ as subfields. Thus any arbitrary field k can always be thought of as a subfield of a Galois number field. It follows from this observation that in our investigation of the properties of algebraic numbers it will be no essential restriction to start with a Galois number field and then show how the factorisation laws for the ideals of such a field carry over to an arbitrary subfield.

First, so far as the proof of the unique factorisation of ideals into prime ideals is concerned, this turns out to be remarkably simple for a Galois number field (*Hilbert* (2, 3)). To examine this let us first fix some notation.

Let K be a Galois number field of degree M, generated by an algebraic integer Θ; then Θ satisfies an irreducible equation of degree M with rational integer coefficients. Let the M roots of this equation be

$$s_1\Theta = \Theta, s_2\Theta, \dots, s_M\Theta,$$

where $s_1, \dots, s_M$ are rational functions of Θ with rational number coefficients. If $s_1, \dots, s_M$ are considered as automorphisms of K they form a group G of order M since of course the successive application of any two of $s_1, \dots, s_M$ must again be one of these automorphisms. G is called the *group of the Galois number field* K. An ideal $\mathfrak{J}$ which remains unaltered when all its members are replaced by their conjugates, i.e. are acted on by any of the $M-1$ automorphisms $s_2, \dots, s_M$, is called an *invariant ideal.* An invariant ideal $\mathfrak{J}$ has the following property.

Lemma 11. *The $M!$-th power of each invariant ideal $\mathfrak{J}$ is equal to a rational integer.*

Proof. Let A be a number in the ideal $\mathfrak{J}$ and let $A_1, A_2, \ldots, A_M$ be the M elementary symmetric functions of $\mathsf{A} = s_1\mathsf{A}, s_2\mathsf{A}, \ldots, s_M\mathsf{A}$. We denote the greatest common divisor of the M rational integers

$$A_1^{M!/1}, A_2^{M!/2}, \ldots, A_M^{M!/M} \tag{10.1}$$

by A. In the same way we form for every other number $\mathsf{B}, \Gamma, \ldots$ of the ideal $\mathfrak{J}$ the corresponding elementary functions and the divisors $B, C, \ldots$. The greatest common divisor of all possible numbers $A, B, C, \ldots$ is denoted by J. Then we claim that $\mathfrak{J}^{M!} = J$. In fact, since all the numbers conjugate to A are also in $\mathfrak{J}$ we have

$$A_1 \equiv 0 \ (\text{mod } \mathfrak{J}), A_2 \equiv 0 \ (\text{mod } \mathfrak{J}^2), \ldots, A_M \equiv 0 \ (\text{mod } \mathfrak{J}^M);$$

consequently all the numbers (10.1) and hence A are congruent to 0 modulo $\mathfrak{J}^{M!}$. Since the same holds likewise for all the numbers $B, C, \ldots$, we have also $J \equiv 0$ modulo $\mathfrak{J}^{M!}$. On the other hand the coefficients $A_1, A_2, \ldots, A_M$ of the M-th degree equation for A are divisible by $J^{1/M!}, J^{2/M!}, \ldots, J^{M/M!}$ respectively and hence A is itself divisible by $J^{1/M!}$. Since the same holds for all the numbers $\mathsf{B}, \Gamma, \ldots$ of the ideal $\mathfrak{J}$ it follows that $\mathfrak{J}^{M!}$ is divisible by J.

As an immediate consequence of Lemma 11 we have the following fact.

Theorem 67. *For each ideal $\mathfrak{A}$ of a Galois number field K there exists an ideal $\mathfrak{B}$ such that the product $\mathfrak{A}\mathfrak{B}$ is a principal ideal.*

Proof. The ideal $\mathfrak{J} = \mathfrak{A} \cdot s_2\mathfrak{A} \cdot \ldots \cdot s_M\mathfrak{A}$ is obviously an invariant ideal. Hence, according to Lemma 11, the ideal

$$\mathfrak{B} = \mathfrak{J}^{(M!-1)} \cdot s_2\mathfrak{A} \cdot \ldots \cdot s_m\mathfrak{A}$$

is an ideal with the property required by Theorem 67.

Theorem 67 allows us to deduce the further divisibility results for the ideals of a Galois number field in the same way as those in Sect. 5 followed from Theorem 8 for an arbitrary number field k.

Now to derive the divisibility laws for an arbitrary field k from those in a Galois number field we may either prove the Kronecker Theorems 13 and 14 on forms first for a Galois number field and deduce that these theorems hold for the subfield k or else apply an appropriate direct transition procedure (*Hilbert* (3)).

§37. Elements, Different and Discriminant of a Galois Number Field

In a Galois number field K many of the concepts introduced earlier have a simpler meaning. Thus the elements of a Galois number field are always ideals of the field itself and indeed we have the following result.

Theorem 68. *The elements of a Galois number field K are permuted by the action of the M automorphisms $s_1, \dots, s_M$. The different $\mathfrak{D}$ of the field K is an invariant ideal and the discriminant $D = \pm N(\mathfrak{D})$, considered as an ideal, is therefore the M-th power of the different $\mathfrak{D}$.*

Proof. Let $\Omega_1, \dots, \Omega_M$ be a basis of the field K. Then the elements of K are ideals

$$\begin{aligned} \mathfrak{E}_2 &= (\Omega_1 - s_2\Omega_1, \dots, \Omega_M - s_2\Omega_M), \\ &\;\;\cdots\cdots\cdots\cdots \\ \mathfrak{E}_M &= (\Omega_1 - s_M\Omega_1, \dots, \Omega_M - s_M\Omega_M). \end{aligned}$$

If we apply any one of the automorphisms s to one of the elements $\mathfrak{E}_i$ and bear in mind that the numbers $s\Omega_1, \dots, s\Omega_M$ also form a basis for the field K then it follows, when we set $ss_i = s_j s$, that

$$s\mathfrak{E}_i = (s\Omega_1 - s_j s\Omega_1, \dots, s\Omega_M - s_j s\Omega_M) = \mathfrak{E}_j.$$

The invariance of the field different follows at once from its representation as $\mathfrak{D} = \mathfrak{E}_2 \dots \mathfrak{E}_M$.

§38. Subfields of a Galois Number Field

In a Galois number field we may undertake a very precise investigation of the decomposition laws for the numbers of the field in relation to its subfields; the results so obtained are of first importance for the application of *general* field theory to *particular* number fields (*Hilbert* (4)).

To give a simple characterization of an arbitrary subfield of a Galois number field we proceed as follows. If the automorphisms $s_1 = 1, s_2, \dots, s_r$ in the group G form a subgroup g of order r then clearly the set of all numbers of the field K which remain unaltered under the action of all the members of g forms a subfield k of K of degree $m = M/r$. This field k is called the *subfield belonging to g*. The Galois field K itself belongs to the group consisting of $s_1 = 1$ alone; the subfield belonging to the group G of all M automorphisms s is the field of rational numbers. Conversely each subfield k of a Galois number field belongs to a certain subgroup g of the group G: g is called the *subgroup fixing k*.

§39. Decomposition Field and Inertia Field of a Prime Ideal

If we take a fixed prime ideal $\mathfrak{P}$ of degree f in a Galois number field K there is a completely determined sequence of subfields of K, ordered by inclusion, which is characteristic of the prime ideal $\mathfrak{P}$ and whose salient properties will now be briefly developed.

Let p be the rational prime divisible by $\mathfrak{P}$; let $z, z', z'', \dots$ be all r_z members of the group G which leave the prime ideal $\mathfrak{P}$ unaltered; these form a group of order r_z which is called the *decomposition group* of $\mathfrak{P}$ and denoted by g_z. The subfield k_z belonging to the decomposition group g_z is called the *decomposition field* of $\mathfrak{P}$; it has degree $m_z = M/r_z$.

Next, let $t, t', t'', \dots$ be all members s of the group G with the property that the congruence $s\Omega \equiv \Omega \pmod{\mathfrak{P}}$ holds for all integers Ω of the field K; let r_t be the number of such automorphisms; it follows easily that they form a group of order r_t. This group is called the *inertia group* of $\mathfrak{P}$ and denoted by g_t. The subfield k_t belonging to g_t is called the *inertia field* of $\mathfrak{P}$; it has degree $m_t = M/r_t$.

The relation between the inertia group and the decomposition group is made clear by the following result.

Theorem 69. *The inertia group g_t of the prime ideal $\mathfrak{P}$ is a normal subgroup of its decomposition group g_z. The members of the decomposition group are each obtained precisely once when we multiply the members of the inertia group by $1, z, z^2, \dots, z^{f-1}$ where z is a suitably chosen member of the decomposition group.*

Proof. Let t be any member of g_t and Ω an integer of K divisible by $\mathfrak{P}$. Set $\Omega' = t^{-1}\Omega$. Then, according to the defining property of the inertia group we have $\Omega' \equiv t\Omega' = \Omega \pmod{\mathfrak{P}}$ and so $\Omega' \equiv 0 \pmod{\mathfrak{P}}$. Application of the automorphism t gives $\Omega \equiv 0$ modulo the prime ideal $t\mathfrak{P}$. Since this congruence holds for every number Ω of the prime ideal $\mathfrak{P}$ it follows that $\mathfrak{P}$ must be divisible by $t\mathfrak{P}$ and consequently $\mathfrak{P} = t\mathfrak{P}$. So the inertia group g_t is a subgroup of the decomposition group g_z.

To prove the remaining assertions of Theorem 69 we choose a primitive root P for the prime ideal $\mathfrak{P}$ which is congruent to 0 modulo all prime ideals conjugate to $\mathfrak{P}$ and distinct from it. The possibility of finding such a primitive root follows from Theorem 25. Then we form the polynomial

$$F(x) = (x - s_1\mathsf{P})(x - s_2\mathsf{P})\dots(x - s_M\mathsf{P})$$

of degree M in x. Since P is a root of the congruence $F(x) \equiv 0 \pmod{\mathfrak{P}}$ it follows from Theorem 27 that P^p also satisfies the same congruence; from this we see that among the M automorphisms $s_1, \dots, s_M$ there must be an automorphism s such that $s\mathsf{P} \equiv \mathsf{P}^p \pmod{\mathfrak{P}}$. If it were the case that

$s^{-1}\mathfrak{P} \neq \mathfrak{P}$ then, according to the choice of P, we have $\mathsf{P} \equiv 0 \pmod{s^{-1}\mathfrak{P}}$ and hence $s\mathsf{P} \equiv 0 \pmod{\mathfrak{P}}$, which contradicts the congruence just established.

Since $s\mathfrak{P} = \mathfrak{P}$ the automorphism s belongs to the decomposition group. We set $s = z$. Repeated application of the automorphism z to the congruence $z\mathsf{P} \equiv \mathsf{P}^p \pmod{\mathfrak{P}}$ leads to the further congruences $z^2\mathsf{P} \equiv \mathsf{P}^{p^2}$, $z^3\mathsf{P} \equiv \mathsf{P}^{p^3}$, $\ldots$, $z^f\mathsf{P} \equiv \mathsf{P}^{p^f} \equiv \mathsf{P} \pmod{\mathfrak{P}}$. It follows from the last congruence that z^f is in the inertia group. Namely, each arbitrary integer Ω of the field K can be represented in the form $\Omega = \mathsf{P}^a + \Pi$ or $\Omega = \Pi$, where a is a rational integer and Π is a number of the field divisible by $\mathfrak{P}$. Since $z^f\mathfrak{P} = \mathfrak{P}$ it follows that we have in fact $z^f\Omega \equiv \Omega \pmod{\mathfrak{P}}$.

The congruence $z\mathsf{P} \equiv \mathsf{P}^p \pmod{\mathfrak{P}}$ shows that $z^{-1}tz\mathsf{P} \equiv \mathsf{P} \pmod{\mathfrak{P}}$ where t is any member of the inertia group g_t. If we set $z' = z^{-1}tz$ and let Ω be an arbitrary integer of the field K then it follows that if Ω satisfies the congruence $\Omega \equiv \mathsf{P}^a \pmod{\mathfrak{P}}$ we have $z'\Omega \equiv (z'\mathsf{P})^a \equiv \mathsf{P}^a \equiv \Omega \pmod{\mathfrak{P}}$ and likewise if $\Omega \equiv 0 \pmod{\mathfrak{P}}$ we have $z'\Omega \equiv \Omega \pmod{\mathfrak{P}}$. Thus $z' = z^{-1}tz$ belongs to the inertia group.

Now let $P(\mathsf{P})$ be any integer polynomial of degree f in P which is congruent to 0 modulo $\mathfrak{P}$. According to Theorem 27 the congruence $P(\mathsf{P}) \equiv 0 \pmod{\mathfrak{P}}$ has the roots $\mathsf{P}, \mathsf{P}^p, \ldots, \mathsf{P}^{p^{f-1}}$ and by Theorem 26 it has no other incongruent roots.

Let z^* be any member of the decomposition group. It follows from the congruence $P(\mathsf{P}) \equiv 0 \pmod{\mathfrak{P}}$ that $P(z^*\mathsf{P}) \equiv 0$ and hence $z^*\mathsf{P} \equiv \mathsf{P}^{p^i}$ where i takes one of the f values $0, 1, \ldots, f-1$. On the other hand $\mathsf{P}^{p^i} \equiv z^i\mathsf{P}$; so we have $z^{-i}z^*\mathsf{P} \equiv \mathsf{P} \pmod{\mathfrak{P}}$ and hence $z^{-i}z^*$ is a member t of the inertia group, i.e. $z^* = z^it$. Thus all the automorphisms $z, z', z'', \ldots$ in the decomposition group can be represented in this form; since, conversely, the automorphisms z^it for $1 = 0, 1, \ldots, f-1$ are all distinct from one another, the last part of Theorem 69 follows. Finally, the fact that the inertia group g_t is a normal subgroup of the decomposition group g_z follows from the result proved above that $z^{-1}tz$ belongs to g_t.

At the same time it follows that $r_z = fr_t$.

§40. A Theorem on the Decomposition Field

The most important property of the decomposition field is described in the following theorem.

Theorem 70. *The ideal* $\mathfrak{p} = \mathfrak{P}^{r_t}$ *belongs to the decomposition field* k_z*, in which it is a prime ideal of degree* 1. *In the decomposition field* k_z *we have* $p = \mathfrak{p}\mathfrak{a}$*, where* $\mathfrak{a}$ *is an ideal prime to* $\mathfrak{p}$.

Proof. The relative norm of the prime ideal $\mathfrak{P}$ with respect to the field k_z is $N_{k_z}(\mathfrak{P}) = \mathfrak{P}^{r_z}$. In order to determine the lowest power of $\mathfrak{P}$ which lies

in k_z, consider the greatest common divisor of all the integers of the field k_z which are divisible by $\mathfrak{P}$. This divisor is necessarily a prime ideal $\mathfrak{p}$ of the field k_z and, since $\mathfrak{P}^{r_z}$ lies in k_z, it follows that $\mathfrak{p}$ must be a power of $\mathfrak{P}$; we set $\mathfrak{p} = \mathfrak{P}^u$. To determine the exponent u we proceed as follows. Let A be a number of the field K not divisible by $\mathfrak{P}$ which satisfies the congruence $\mathsf{A} \equiv z\mathsf{A} \pmod{\mathfrak{P}}$; if $\mathsf{A} \equiv \mathsf{P}^i \pmod{\mathfrak{P}}$ then we must have $i \equiv pi \pmod{p^f - 1}$ and so i must be divisible by $1+p+p^2+\cdots+p^{f-1}$. Thus there are only $p-1$ numbers mutually incongruent modulo $\mathfrak{P}$ which have the desired property. It follows that $\mathsf{A} \equiv a \pmod{\mathfrak{P}}$, where a is a rational integer. From these considerations it follows in particular that every number α of the field k_z is congruent to a rational number modulo $\mathfrak{P}$, and hence also modulo $\mathfrak{p}$. Thus $\mathfrak{p}$ is a prime ideal in k_z of degree 1 and consequently the norm $n(\mathfrak{p})$ in the field k_z is p. On the other hand the norm of $\mathfrak{p}$ in the field K is given by the formula $N(\mathfrak{p}) = (n(\mathfrak{p}))^{r_z}$. Since $\mathfrak{p} = \mathfrak{P}^u$ and $N(\mathfrak{P}) = p^f$ it follows that $p^{uf} = p^{r_z}$ and so $u = r_t$.

From the definition of the decomposition group it follows that $N(\mathfrak{P}) = \mathfrak{P}^{r_z}\mathfrak{A}$ where $\mathfrak{A}$ is an ideal prime to $\mathfrak{P}$. If we set $p = \mathfrak{p}\mathfrak{a}$ we have $N(\mathfrak{P}) = p^f = \mathfrak{p}^f\mathfrak{a}^f$ and consequently $\mathfrak{a}^f = \mathfrak{A}$, whence the last part of Theorem 70 is proved.

§41. The Ramification Field of a Prime Ideal

To investigate the structure of the inertia group more closely we take a fixed number A of the field K which is divisible by $\mathfrak{P}$ but not by $\mathfrak{P}^2$ and examine for all the members $t, t', t'', \ldots$ of the inertia group the congruences

$$\left.\begin{array}{rcl} t\mathsf{A} & \equiv & \mathsf{P}^a\mathsf{A} \\ t'\mathsf{A} & \equiv & \mathsf{P}^{a'}\mathsf{A} \\ t''\mathsf{A} & \equiv & \mathsf{P}^{a''}\mathsf{A} \\ & \cdots\cdots & \end{array}\right\} \pmod{\mathfrak{P}^2}$$

where $a, a', a'', \ldots$ are numbers in the sequence $0, 1, 2, \ldots, p^f - 2$. We denote the automorphisms $t, t', t'', \ldots$ for which the corresponding exponents $a, a', a'', \ldots$ have the value 0 by $v, v', v'', \ldots$. We suppose there are r_v of them; they form, as is easily seen, a normal subgroup of the inertia group. This subgroup of order r_v is called the *ramification group* of the prime ideal $\mathfrak{P}$ and is denoted by g_v. The subfield k_v belonging to g_v is called the *ramification field* of the prime ideal $\mathfrak{P}$. The relation of the ramification group to the inertia group is described more precisely by the following theorem.

Theorem 71. *The ramification group g_v is a normal subgroup of the inertia group. The order r_v of the ramification group is a power of p, say $r_v = p^l$. The members of the inertia group are obtained (each one uniquely) when we multiply the members of the ramification group by 1, t, $t^2, \ldots, t^{h-1}$,*

where $h = r_t/r_v$ and t is a suitably chosen member of the inertia group. The number h is a divisor of $p^f - 1$.

Proof. Let $\mathfrak{P}^u$ be a sufficiently high power of $\mathfrak{P}$ that for every member v of the ramification group other than the identity we have $v\mathsf{A} \not\equiv \mathsf{A} \pmod{\mathfrak{P}^u}$. If we set $v\mathsf{A} \equiv \mathsf{A} + \mathsf{B}\mathsf{A}^2 \pmod{\mathfrak{P}^3}$, where B is an integer in K then it follows easily that $v^p\mathsf{A} \equiv \mathsf{A} \pmod{\mathfrak{P}^3}$ and similarly $v^{p^2}\mathsf{A} \equiv \mathsf{A} \pmod{\mathfrak{P}^4}$ and so on. Finally we have $v^{p^{u-2}}\mathsf{A} \equiv \mathsf{A} \pmod{\mathfrak{P}^u}$. Hence $v^{p^{u-2}} = 1$; thus the order r_v of the ramification group is a power of p, say $r_v = p^l$.

Now let a be the smallest of the nonzero exponents $a, a', a'', \ldots$. Suppose there are in all h distinct exponents. Then they are necessarily all multiples of a and they coincide with the numbers $0, a, 2a, \ldots, (h-1)a$; furthermore $ha = p^f - 1$. At the same time we recognise that all the members of the inertia group can be expressed in the form $t^i v$ where i takes the values $0, 1, \ldots, h-1$ and v runs through all the members of the ramification group g_v. It follows that $r_t = hr_v$.

§42. A Theorem on the Inertia Field

The following theorem provides information about the behaviour of the ideals $\mathfrak{p}$ and $\mathfrak{P}$ in the field k_t.

Theorem 72. *Every number of the field K is congruent modulo $\mathfrak{P}$ to a number in the inertia field. The inertia field effects no decomposition of the ideal $\mathfrak{p}$, but only an increase in its degree; namely, on passing from the field k_z to the higher field k_t, the ideal $\mathfrak{p}$ changes from a prime ideal of degree 1 to a prime ideal of degree f.*

Proof. We set

$$\begin{aligned}\pi &= \{v\mathsf{P} \cdot v'\mathsf{P} \cdot v''\mathsf{P} \cdots\}^{p^{l(f-1)}},\\ \kappa &= (\pi + t\pi + t^2\pi + \cdots + t^{h-1}\pi)/h,\end{aligned}$$

where P is again a primitive root for $\mathfrak{P}$ and t is the automorphism chosen in Theorem 71. The number π lies in the field k_v and κ lies in the field k_t. To prove the latter statement we notice that κ remains unaltered under the automorphism t since t^h belongs to g_v and that the numbers $\pi, t\pi, t^2\pi, \ldots, t^{h-1}\pi$ remain unaltered under any automorphism in g_v. We see easily that both π and κ are congruent modulo $\mathfrak{P}$ to the primitive root P. It follows that there are precisely p^f numbers in k_t mutually incongruent modulo $\mathfrak{P}$; hence $\mathfrak{p} = \mathfrak{P}^{r_t}$ does not split in the field k_t and consequently in k_t it is a prime ideal of degree f.

§43. Theorems on the Ramification Group and Ramification Field

It is now easy to recognise the characteristic property of the ramification group: it is the following.

Theorem 73. *The ramification group consists precisely of the automorphisms s such that $s\Omega \equiv \Omega \pmod{\mathfrak{P}^2}$ for all integers Ω of K*

Proof. Let Ω be any number of K; suppose Ω is congruent modulo $\mathfrak{P}$ to the number ω in the inertia field. Then we have $\Omega - \omega \equiv \mathsf{BA} \pmod{\mathfrak{P}^2}$ where A has the same meaning as in Sect. 41 and B is a suitably chosen integer of K. Applying an automorphism v in the ramification group we have $v\Omega - \omega \equiv v(\mathsf{BA}) \equiv \mathsf{BA} \equiv \Omega - \omega \pmod{\mathfrak{P}^2}$; so $v\Omega \equiv \Omega \pmod{\mathfrak{P}^2}$.

At the same time we have the following further result on the ramification field.

Theorem 74. *The ideal $\mathfrak{p}_v = \mathfrak{P}^{r_v}$ lies in the ramification field where it is a prime ideal of degree f. In the ramification field the ideal $\mathfrak{p}$ splits as a product of h equal prime factors $\mathfrak{p} = \mathfrak{p}_v^h$.*

§44. Higher Ramification Groups of a Prime Ideal

Our next task is to investigate more closely the splitting of the ideal $\mathfrak{p}_v$ into equal factors.

To this end let L be the highest exponent such that for every member v of the ramification group and every integer Ω in K we have $v\Omega \equiv \Omega \pmod{\mathfrak{P}^L}$. Then all the automorphisms s in the ramification group such that $s\Omega \equiv \Omega \pmod{\mathfrak{P}^{L+1}}$ for all integers Ω of K form a subgroup $g_{\bar{v}}$ of the ramification group, which we call the *first higher ramification group* of the prime ideal $\mathfrak{P}$. The subfield $k_{\bar{v}}$ belonging to $g_{\bar{v}}$ is called the *first higher ramification field* of $\mathfrak{P}$. The most important property of this field is the following.

Theorem 75. *The first higher ramification group $g_{\bar{v}}$ is a normal subgroup of the ramification group g_v. Let the order of $g_{\bar{v}}$ be $r_{\bar{v}} = p^{\bar{l}}$. Then the members of the ramification group g_v are obtained (each one uniquely) when we multiply the members of $g_{\bar{v}}$ by $p^{\bar{e}}$ suitably chosen members $v_1, \ldots, v_{p^{\bar{e}}}$ of the ramification group g_v; these $p^{\bar{e}}$ automorphisms have the property that for any two of them, v_i and $v_{i'}$, there always exists a relation of the form $v_i v_{i'} = v_{i'} v_i \bar{v}$ where $\bar{v}$ is a member of $g_{\bar{v}}$. The ideal $\mathfrak{p}_{\bar{v}} = \mathfrak{P}^{r_{\bar{v}}}$ is a prime ideal in $k_{\bar{v}}$; thus in $k_{\bar{v}}$ the ideal $\mathfrak{p}_v$ splits as a product of $p^{\bar{e}}$ equal prime factors: $\mathfrak{p}_v = \mathfrak{p}_{\bar{v}}^{p^{\bar{e}}}$; moreover the exponent $\bar{e}$ does not exceed the degree f of $\mathfrak{P}$.*

Proof. Let A be an integer of the field K which is divisible by $\mathfrak{P}$ but not by $\mathfrak{P}^2$. Then we determine a set of members $v_1, \ldots, v_r$ of the ramification group such that when we set

$$v_1\mathsf{A} \equiv \mathsf{A} + \mathsf{B}_1\mathsf{A}^L, \ldots, v_r\mathsf{A} \equiv \mathsf{A} + \mathsf{B}_r\mathsf{A}^L \pmod{\mathfrak{P}^{L+1}},$$

the integers $\mathsf{B}_1, \ldots, \mathsf{B}_r$ are all incongruent to one another modulo $\mathfrak{P}$ and further no other member of g_v can be added to the set $g_1, \ldots, g_r$ without infringing the latter condition. Now choose an arbitrary member v^* of the ramification group g_v and set $v^*\mathsf{A} \equiv \mathsf{A} + \mathsf{B}\mathsf{A}^L \pmod{\mathfrak{P}^{L+1}}$, so that B must be congruent modulo $\mathfrak{P}$ to one of the numbers $\mathsf{B}_1, \ldots, \mathsf{B}_r$, say $\mathsf{B} \equiv \mathsf{B}_i \pmod{\mathfrak{P}}$. Then $v_i^{-1}v^*\mathsf{A} \equiv \mathsf{A} \pmod{\mathfrak{P}^{L+1}}$. It follows from Theorem 72 that each integer Ω of K is congruent modulo $\mathfrak{P}^{L+1}$ to an expression of the form $\alpha_t + \beta_t\mathsf{A} + \cdots + \lambda_t\mathsf{A}^L$ where $\alpha_t, \beta_t, \ldots, \lambda_t$ are integers of the inertia field. It follows that Ω satisfies the congruence $v_i^{-1}v^*\Omega \equiv \Omega \pmod{\mathfrak{P}^{L+1}}$; so we have $v_i^{-1}v^* = \bar{v}$ or $v^* = v_i\bar{v}$. This equation establishes the structure of the group $g_{\bar{v}}$ asserted in Theorem 75.

We set $r_{\bar{v}} = p^{\bar{l}}$ and $\bar{e} = l - \bar{l}$.

It is now clear how to continue with the procedure we have started on. Let $\bar{L}$ be the highest exponent such that $\bar{v}\Omega \equiv \Omega \pmod{\mathfrak{P}^{\bar{L}}}$ for all numbers Ω of the field K and all members $\bar{v}$ of $g_{\bar{v}}$. Then we determine all the automorphisms $\bar{\bar{v}}$ such that $\bar{\bar{v}}\Omega \equiv \Omega \pmod{\mathfrak{P}^{\bar{L}+1}}$ for all Ω. These form a normal subgroup $g_{\bar{\bar{v}}}$ of the group $g_{\bar{v}}$; we call it the *second higher ramification group* of the prime ideal $\mathfrak{P}$. If its order is $r_{\bar{\bar{v}}} = p^{\bar{\bar{l}}}$ we set $\bar{\bar{e}} = \bar{l} - \bar{\bar{l}}$; then $\mathfrak{p}_{\bar{v}} = \mathfrak{p}_{\bar{\bar{v}}}^{\bar{\bar{e}}}$ where $\mathfrak{p}_{\bar{\bar{v}}}$ is a prime ideal of the subfield $k_{\bar{\bar{v}}}$ belonging to $g_{\bar{\bar{v}}}$.

Continuing in this way we reach the *third higher ramification group* of the prime ideal $\mathfrak{P}$ and so on. If the i-th higher ramification group of $\mathfrak{P}$ is the first which consists of the identity substitution 1 alone the i-th higher ramification field of $\mathfrak{P}$ is the field K itself and the structure of the ramification group g_v is completely determined. It is clear that higher ramification groups of a prime ideal $\mathfrak{P}$ can occur only if the degree M of the field K is divisible by p.

§45. Summary of the Theorems on the Decomposition of a Rational Prime Number p in a Galois Number Field

By means of the theorems developed in Sect. 39-44 we obtain a complete picture of the procedure followed in the decomposition of a rational prime number in a Galois number field. If we concern ourselves with a particular prime ideal factor $\mathfrak{P}$ of p we have first the result that p splits in the decomposition field of $\mathfrak{P}$ in the form $p = \mathfrak{p}\mathfrak{a}$ where $\mathfrak{p}$ is a prime ideal of degree 1 and $\mathfrak{a}$ is an ideal of the decomposition field not divisible by $\mathfrak{p}$. The decomposition field of $\mathfrak{P}$ is a subfield of the inertia field of $\mathfrak{P}$, which for its part effects no further factorisation of $\mathfrak{p}$ but merely expands it to a prime ideal of degree f.

If K is itself either the decomposition field or the inertia field of $\mathfrak{P}$ then the decomposition of p is completed at this first stage. Otherwise $\mathfrak{p}$ splits into equal factors in K; first of all $\mathfrak{p}$ becomes in the ramification field a power of a prime ideal $\mathfrak{p}_v$ with exponent dividing $p^f - 1$ and hence not divisible by p. The splitting of $\mathfrak{p}$ is completed at this second stage if and only if p does not divide the order of the inertia group and so K is itself the ramification field. In the higher ramification fields, if any, the splitting continues without interruption, the corresponding exponents being numbers of the form $p^{\bar{e}}$, $p^{\bar{\bar{e}}}$, $\ldots$, where none of the exponents $\bar{e}$, $\bar{\bar{e}}$, $\ldots$ exceeds the degree f of the prime ideal $\mathfrak{P}$.

This survey of the results we have developed is more clearly illustrated by the following table in which the rows show for each field successively the order of its group, its degree, its relative degree with respect to the next lower field and its prime ideal with its representation as a power of $\mathfrak{P}$.

k_z	k_t	k_v	$k_{\bar{v}}$	$k_{\bar{\bar{v}}}$	K
r_z	r_t	r_v	$r_{\bar{v}}$	$r_{\bar{\bar{v}}}$	1
$m_z = \frac{M}{r_z}$	$m_t = \frac{M}{r_t}$	$m_v = \frac{M}{r_v}$	$m_{\bar{v}} = \frac{M}{r_{\bar{v}}}$	$m_{\bar{\bar{v}}} = \frac{M}{r_{\bar{\bar{v}}}}$	M
	$f = \frac{r_z}{r_t}$	$h = \frac{r_t}{r_v}$	$p^{\bar{e}} = \frac{r_v}{r_{\bar{v}}}$	$p^{\bar{\bar{e}}} = \frac{r_{\bar{v}}}{r_{\bar{\bar{v}}}}$	$p^{\bar{\bar{\bar{e}}}} = r_{\bar{\bar{v}}}$
$\mathfrak{p} = \mathfrak{p}_v^h = \mathfrak{P}^{r_t}$		$\mathfrak{p}_v = \mathfrak{p}_{\bar{v}}^{p^{\bar{e}}} = \mathfrak{P}^{r_v}$	$\mathfrak{p}_{\bar{v}} = \mathfrak{p}_{\bar{\bar{v}}}^{p^{\bar{\bar{e}}}} = \mathfrak{P}^{r_{\bar{v}}}$	$\mathfrak{p}_{\bar{\bar{v}}} = \mathfrak{p}_{\bar{\bar{\bar{v}}}}^{p^{\bar{\bar{\bar{e}}}}} = \mathfrak{P}^{r_{\bar{\bar{v}}}}$	$\mathfrak{P}$

The field K is here taken to coincide with the third higher ramification field. All the degrees and exponents appearing in the table have the same value for all the prime ideals $\mathfrak{P}$ of the field K which divide p and are thus completely determined by the prime number p alone.

11. The Differents and Discriminants of a Galois Number Field and its Subfields

§46. The Differents of the Inertia Field and the Ramification Field

A rich source of new results is opened up if we bring together the results we have just obtained with those of Chap. 5. Thus, by using Theorem 41, we easily obtain a theorem which states the most important property of the inertia field; it runs as follows.

Theorem 76. *The different of the inertia field of the prime ideal $\mathfrak{P}$ is not divisible by $\mathfrak{P}$. The inertia field includes all the subfields of K for which the different is not divisible by $\mathfrak{P}$.*

Concerning the different of the ramification field we have the following theorems.

Theorem 77. *The relative different of the ramification field with respect to the inertia field is divisible by $\mathfrak{P}^{r_t - r_v} = \mathfrak{p}_v^{h-1}$ and by no higher power of $\mathfrak{P}$.*

Proof. According to Theorem 41 we have $\mathfrak{D}_t(K) = \mathfrak{D}_v(K)\mathfrak{d}_t(k_v)$ where $\mathfrak{D}_t(K)$, $\mathfrak{D}_v(K)$ and $\mathfrak{d}_t(k_v)$ are respectively the relative differents of K with respect to k_t, K with respect to k_v and k_v with respect to k_t. If Ξ is the fundamental form of K it follows from this that the content of the form $\prod(\Xi - t\Xi)$ is equal to the product of the content of the form $\prod(\Xi - v\Xi)$ and $\mathfrak{d}_t(k_v)$, where in the first product t runs through all the automorphisms in the inertia group and in the second v runs through all the automorphisms in the ramification group. All the factors $\Xi - v\Xi$ occur among the $\Xi - t\Xi$; according to the definition of the ramification group the remaining factors are all divisible by $\mathfrak{P}$ but by no higher power of $\mathfrak{P}$. The assertion of the theorem follows from the fact that $r_t - r_v = (h-1)r_v$.

Similarly we have the following result.

Theorem 78. *The relative different of the first higher ramification field $k_{\bar{v}}$ with respect to the ramification field k_v is divisible by $\mathfrak{P}^{L(r_v - r_{\bar{v}})} = \mathfrak{p}_{\bar{v}}^{L(p^{\bar{e}}-1)}$ precisely. The relative different of the second higher ramification field $k_{\bar{\bar{v}}}$ with respect to $k_{\bar{v}}$ is divisible by $\mathfrak{P}^{\bar{L}(r_{\bar{v}} - r_{\bar{\bar{v}}})} = \mathfrak{p}_{\bar{\bar{v}}}^{\bar{L}(p^{\bar{e}}-1)}$ precisely and so on.*

§47. The Divisors of the Discriminant of a Galois Number Field

Theorem 79. *The exponent of the power to which the rational prime p occurs as a factor of the discriminant D of the field K is*

$$m_t\{r_t - r_v + L(r_v - r_{\bar{v}}) + \bar{L}(r_{\bar{v}} - r_{\bar{\bar{v}}}) + \cdots\}.$$

Proof. Theorem 41 taken together with Theorems 76, 77 and 78 shows that the different $\mathfrak{D}$ of the field K contains the prime ideal $\mathfrak{P}$ to the $(r_t - r_v + L(r_v - r_{\bar{v}}) + \bar{L}(r_{\bar{v}} - r_{\bar{\bar{v}}}) + \cdots)$-th power precisely. The assertion of Theorem 79 now follows by Theorem 68.

In the case where no higher ramification fields are present the term involving L does not appear and it follows that the exponent of the power of p dividing D has the value $m_t(r_t - 1)$. According to what we have seen earlier this case certainly occurs when the degree M is prime to p. (Compare the remarks at the end of Sect. 12.)

Theorem 80. *The exponent of the power of a rational prime p which divides the discriminant D does not exceed a certain bound which depends only on the degree M of the Galois number field K.*

Proof. We claim that all the exponents L, $\bar{L}$, ... for a prime ideal $\mathfrak{P}$ are less than a bound determined by M alone.

To find such a bound for L we denote by ω an integer of $k_{\bar{v}}$ divisible by $\mathfrak{p}_{\bar{v}}$ but not by $\mathfrak{p}_{\bar{v}}^2$ and choose $p^{\bar{e}}$ members $v_1, v_2, \ldots, v_{p^{\bar{e}}}$ of the ramification group g_v which together with $g_{\bar{v}}$ generate g_v. The number $\alpha = v_1\omega + v_2\omega + \cdots + v_{p^{\bar{e}}}\omega$ remains unaltered under all the automorphisms in g_v and hence belongs to the field k_v. On the other hand we have $\omega \equiv v\omega \pmod{\mathfrak{P}^L}$ for all automorphisms v in the ramification group and hence $\alpha \equiv p^{\bar{e}}\omega \pmod{\mathfrak{P}^L}$. If we had $L > \bar{e}r_t + r_{\bar{v}}$ then we would have $\alpha \equiv 0 \pmod{\mathfrak{p}^{\bar{e}}\mathfrak{p}_{\bar{v}}}$ but $\not\equiv 0 \pmod{\mathfrak{p}^{\bar{e}}\mathfrak{p}_{\bar{v}}\mathfrak{P}}$. Setting $p = \mathfrak{p}\mathfrak{a}$, where $\mathfrak{a}$ is an ideal of the decomposition field prime to $\mathfrak{p}$, and taking γ to be a number of the decomposition field divisible by $\mathfrak{a}$ and prime to $\mathfrak{p}$, we see that $\beta = \alpha\gamma^{\bar{e}}/p^{\bar{e}}$ is an integer in $k_{\bar{v}}$; β is divisible by $\mathfrak{p}_{\bar{v}}$ but not by $\mathfrak{p}_{\bar{v}}\mathfrak{P}$. From this it follows that $\mathfrak{p}_{\bar{v}}$ is an ideal of the field k_v, in contradiction to Theorem 75. Since we can in a similar way find upper bounds for the

remaining exponents $\bar{L}, \ldots$, it follows that the exponent given in Theorem 79 for the power of p which divides the discriminant D cannot exceed a certain bound which depends only on the degree M of the field K.

Theorem 80 is important especially because it restricts to a *finite* number the possibilities which can occur for the behaviour of the prime divisors of M. If we count as a single type all the fields of degree M for which all the above numbers associated with the decomposition of all the prime numbers dividing M have the same value then it follows that for a given degree M there are only *finitely* many possible types.

As an example of Theorem 80 we mention the quadratic fields (studied in detail in Part III), in which the discriminant is divisible by at most the first power of each odd prime and by at most the third power of the prime 2 (see Sect. 59, Theorem 95).

12. Connexion Between the Arithmetic and Algebraic Properties of a Galois Number Field

§48. Galois, Abelian and Cyclic Extension Fields

If the group G of automorphisms $s_1, \ldots, s_M$ of a Galois number field K is an abelian group, i.e. if the automorphisms $s_1, \ldots, s_M$ commute with one another, then K is called an *abelian field.* In particular, if the group G is cyclic, i.e. if all M automorphisms $s_1, \ldots, s_M$ can be represented as powers of a single one of them, then the abelian field K is called a *cyclic field.*

If we apply to the group of automorphisms of an abelian field the same arguments as we used in Sect. 28 for the ideal classes, we derive the result that every abelian field can be composed of cyclic fields. The cyclic fields for their part can be composed of special cyclic fields whose degrees are prime numbers or powers of a prime number.

The concepts we have been discussing can be generalised in the following way.

Let Θ be a root of an equation of degree l,

$$\Theta^l + \alpha_1\Theta^{l-1} + \cdots + \alpha_l = 0,$$

whose coefficients $\alpha_1, \ldots, \alpha_l$ are numbers of a field k of degree m. Suppose further that this l-th degree equation is irreducible over the field k and that all its remaining $l-1$ roots, $\Theta', \ldots, \Theta^{(l-1)}$ can be represented as polynomials in the root Θ with coefficients in the field k. Under these assumptions we call the algebraic number field K of degree $M = lm$ generated by Θ and the numbers in k a *Galois extension* of k. The degree l of the equation is the *degree of* K *over* k. If we set

$$\Theta = S_1\Theta, \Theta' = S_2\Theta, \ldots, \Theta^{(l-1)} = S_l\Theta$$

then the automorphisms $S_1, \ldots, S_l$ form the *group of* K *over* k. If this group is abelian we say that K is an *abelian extension* of k; if the group is cyclic, K is called a *cyclic extension* of k.

§49. Algebraic Properties of the Inertia Field and the Ramification Field. Representation of the Numbers of a Galois Number Field by Radicals over the Decomposition Field

Using the notions defined above we may derive very easily several important properties of the decomposition field, the inertia field and the ramification fields which are immediate consequences of the properties of their groups which we proved earlier. We have the following results.

Theorem 81. *The inertia field k_t is a cyclic extension of degree f over the decomposition field k_z. The ramification field k_v is a cyclic extension of degree h over the inertia field k_t. The first higher ramification field $k_{\bar{v}}$ is an abelian extension of degree $p^{\bar{e}}$ over the ramification field k_v; the field $k_{\bar{\bar{v}}}$ is an abelian extension of degree $p^{\bar{\bar{e}}}$ over $k_{\bar{v}}$. The abelian groups of $k_{\bar{v}}$ over k_v, $k_{\bar{\bar{v}}}$ over $k_{\bar{v}}$, ... all consist entirely of automorphisms of order p.*

According to Theorem 81 we see that the splitting of a prime ideal into *equal* factors always takes place by means of a sequence of abelian equations; this result leads to a new surprising property of the decomposition field.

Theorem 82. *For each prime ideal $\mathfrak{P}$ of a Galois number field K the numbers in K can be expressed by means of radicals over the decomposition field of $\mathfrak{P}$, i.e. K is a radical extension of the decomposition field of each of its prime ideals.*

Theorem 82 shows clearly the significance of the theory of equations solvable by radicals; for it shows that in the process of decomposing numbers into prime ideals the most important and most difficult steps occur in extension fields whose numbers are representable by radicals over a certain subfield.

§50. The Density of Prime Ideals of Degree 1 and the Connexion Between this Density and the Algebraic Properties of a Number Field

It is a remarkable fact that the distribution of certain prime ideals of degree 1 in a number field allows us to draw conclusions concerning the algebraic properties of the field (*Kronecker* (14)).

Let k be an arbitrary number field of degree m; let p_i denote the general rational prime number which is divisible by precisely i distinct prime ideals of degree 1. Consider the function

$$\frac{\sum\limits_{(p_i)} p_i^{-s}}{\log\left(\frac{1}{s-1}\right)},$$

(where the sum in the numerator is taken over all the prime numbers p_i). If this function has a limit at $s = 1$ we say that the prime numbers of type p_i have a density; if the limit is Δ_i then we call Δ_i the *density* of the prime numbers of type p_i. Kronecker in the course of his investigations made the tacit assumption that the prime numbers of types $p_1, \ldots, p_m$ all have densities. For the case where the group of the equation which serves to define the field k is symmetric we can deduce already from Kronecker's remarks the existence of the densities $\Delta_1, \ldots, \Delta_m$. Frobenius proved the existence of these densities for an arbitrary field k and also determined their values; they are rational numbers which depend in a simple way on the group of the equation which determines the field k (*Frobenius* (1)). We easily obtain the proof of the following theorem.

Theorem 83. *Suppose that in an arbitrary field of degree m any $m-1$ of the prime number types $p_1, \ldots, p_m$ have densities. Then so also does the remaining type and the m densities $\Delta_1, \ldots, \Delta_m$ satisfy the relation*

$$\Delta_1 + 2\Delta_2 + \cdots + m\Delta_m = 1.$$

Proof. If we use the second of the three representations of the function $\zeta(s)$ given in Sect. 27 and take logarithms we have

$$\log\zeta(s) = \sum_{(\mathfrak{p})} n(\mathfrak{p})^{-s} + S,$$

$$S = \frac{1}{2}\sum_{(\mathfrak{p})} n(\mathfrak{p})^{-2s} + \frac{1}{3}\sum_{(\mathfrak{p})} n(\mathfrak{p})^{-3s} + \ldots,$$

where the sums are taken over all the prime ideals $\mathfrak{p}$ of the field. We denote by $\mathfrak{p}_1$ the general prime ideal of degree 1; then it is clear that

$$\sum_{(\mathfrak{p}_1)} n(\mathfrak{p}_1)^{-s} = \sum_{(p_1)} p_1^{-s} + \sum_{(p_2)} 2p_2^{-s} + \cdots + \sum_{(p_m)} mp_m^{-s}, \tag{12.1}$$

where the sum on the left is taken over all prime ideals $\mathfrak{p}_1$ and those on the right over all rational primes $p_1, p_2, \ldots, p_m$ respectively.

When we bear in mind on the other hand that for all prime ideals $\mathfrak{p}$ of degree greater than 1 we have $n(\mathfrak{p}) \geq p^2$ and that an arbitrary prime number p is divisible by at most m prime ideals it follows that

$$\sum_{(\mathfrak{p})} n(\mathfrak{p})^{-s} - \sum_{(\mathfrak{p}_1)} n(\mathfrak{p}_1)^{-s} \leq m\sum_{(p)} p^{-2s} < m\sum_{(h)} h^{-2},$$

where the last sum is taken over all rational integers h greater than 1. Similarly we find that

$$S < m\left\{\sum_{(h)}\frac{1}{h^2}+\sum_{(h)}\frac{1}{h^3}+\cdots\right\} = m\sum_{(h)}\frac{1}{h(h-1)} = m.$$

From these inequalities it follows that

$$\log\zeta(s) - \sum_{(\mathfrak{p}_1)} n(\mathfrak{p}_1)^{-s}$$

has a finite limit at $s = 1$. According to Theorem 56,

$$\log\zeta(s) - \log\left(\frac{1}{s-1}\right)$$

has a finite limit at $s = 1$; so the same is true of

$$\sum_{(\mathfrak{p}_1)} n(\mathfrak{p}_1)^{-s} - \log\left(\frac{1}{s-1}\right),$$

whence

$$\lim_{s=1}\frac{\sum_{(\mathfrak{p}_1)} n(\mathfrak{p}_1)^{-s}}{\log\left(\frac{1}{s-1}\right)} = 1$$

and the assertion of Theorem 83 follows by means of the formula (12.1).

For a Galois number field K of degree M we have $\Delta_1 = 0$, $\Delta_2 = 0$, ..., $\Delta_{M-1} = 0$, and so we have the following consequence of Theorem 83.

Theorem 84. *The prime numbers p_M which split completely as products of prime ideals of degree 1 in a Galois number field of degree M have a density and this density is $\Delta_M = 1/M$.*

If k is an arbitrary number field and K is the Galois number field of degree M formed by the composition of k and its conjugate fields k', ..., $k^{(m-1)}$ then, as is easily seen, the prime numbers p_m in k coincide with the prime numbers p_M in K. Hence the prime numbers p_m in k have a density and this density is $1/M$, i.e. the reciprocal of the degree of the Galois closure of k (*Kronecker* (14)).

13. Composition of Number Fields

§51. The Galois Number Field Formed by the Composition of a Number Field and its Conjugates

Theorem 85. *If K is the compositum of two number fields k_1 and k_2 then the discriminant of K is divisible by all those rational prime numbers which divide the discriminant of k_1 or the discriminant of k_2 or both and only by those prime numbers.*

The first part of this theorem follows immediately from Theorem 39; the second part can be obtained as a consequence of Theorem 41 as follows.

Let $\Omega_1, \ldots, \Omega_M$ and $\omega_1, \ldots, \omega_m$ be bases for K and k_1 respectively. Then the numbers ω_i $(i = 1, \ldots, m)$ can be represented in the form

$$\omega_i = a_{i1}\Omega_1 + \ldots + a_{im}\Omega_M,$$

where $a_{i1}, \ldots, a_{iM}$ are rational integers. Let $\Omega_1^{(l)}, \ldots, \Omega_M^{(l)}$ be the conjugates of $\Omega_1, \ldots, \Omega_M$ with respect to k_2; then the numbers

$$\omega_i^{(l)} = a_{i1}\Omega_1^{(l)} + \ldots + a_{im}\Omega_M^{(l)},$$

are certain conjugates of ω_i and it follows that the element

$$(\Omega_1 - \Omega_1^{(l)}, \ldots, \Omega_M - \Omega_M^{(l)})$$

of K divides certain elements of k. The assertion of the theorem follows from the definition of the relative different and Theorem 38.

An immediate consequence of Theorem 85 is the following fact.

Theorem 86. *Let k be a number field of degree m; let K be the Galois number field formed by the composition of k and its conjugates $k', \ldots, k^{(m-1)}$. Then the discriminant of K is divisible by precisely those rational prime numbers which divide the discriminant of k.*

§52. Compositum of Two Fields Whose Discriminants Are Relatively Prime

Of particular interest is the case in which the discriminants of the fields forming the compositum are relatively prime. The most important and productive result in this case is the following.

Theorem 87. *If k_1 and k_2 are number fields of degrees m_1 and m_2 respectively whose discriminants are relatively prime then their compositum is a field of degree $m_1 m_2$.*

Proof. We denote by K_1 the Galois number field formed by composing k_1 and all its conjugates; according to Theorem 86 the discriminant of K_1 is relatively prime to the discriminant of k_2. Let ϑ be a generator of the field k_1; ϑ satisfies an irreducible equation of degree m_1 with rational integer coefficients.

If the compositum of k_1 and k_2 were of degree less than $m_1 m_2$ this equation would be reducible over k_2, i.e. ϑ would satisfy an equation of the form

$$\vartheta^r + \alpha_1 \vartheta^{r-1} + \cdots + \alpha_r = 0$$

with degree r less than m_1 and coefficients $\alpha_1, \ldots, \alpha_r$ in k_2. We denote by k the number field generated by these coefficients $\alpha_1, \ldots, \alpha_r$. Since $\alpha_1, \ldots, \alpha_r$ can be expressed rationally in terms of the roots of the above equation it follows that k is a subfield of K_1. Since k is also a subfield of k_2 it follows from Theorem 39 that the discriminant of k must be a factor both of the discriminant of k_1 and of the discriminant of k_2; from this we deduce that the discriminant of k is 1 and this contradicts Theorem 44.

We emphasize here the following facts, the truth of which can now be easily established.

Theorem 88. *If k_1 and k_2 are fields of degrees m_1 and m_2 respectively with relatively prime discriminants d_1 and d_2 respectively then the discriminant of their compositum K is $d_1^{m_2} d_2^{m_1}$. We obtain the $m_1 m_2$ members of a basis for the field K by multiplying the m_1 members of a basis for k_1 by the m_2 members of a basis for k_2. If p is a rational prime number which factorises in k_1 as $p = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r}$ and in k_2 as $p = \mathfrak{q} \ldots \mathfrak{q}_s$ where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ are distinct prime ideals of k_1, k_2 respectively, then p factorises in K as $p = \prod_{i,l} \mathfrak{J}_{il}^{e_i}$ where the product is taken over $i = 1, \ldots, r$ and $l = 1, \ldots, s$ and $\mathfrak{J}_{il}$ is the greatest common divisor of $\mathfrak{p}_i$ and $\mathfrak{q}_l$ in K. The ideals $\mathfrak{J}_{il}$ are not necessarily prime ideals in K.*

If the fields k_1 and k_2 have arbitrary discriminants then the corresponding questions admit simple answers only under restrictive hypotheses on the nature of the prime numbers to be factorised (*Hensel* (3)).

The results described thus far in Chapters 10 to 13 seem to me to comprise the most important features of a theory of ideals and discriminants of Galois number fields. The methods we have used allow a more general development in several directions; in particular we have a series of theorems similar to those proved in Sect. 39-44 which hold without essential alteration for Galois extension fields (*Dedekind* (8)).

14. The Prime Ideals of Degree 1 and the Class Concept

§53. Generation of Ideal Classes by Prime Ideals of Degree 1

It is very interesting that the principles developed in Chapters 10 to 12 also throw new light on the question of the generation and constitution of the ideal classes of a number field. In this and the following chapter we shall describe the most important general theorems concerning this matter. The first theorem concerns the generation of the ideal classes of an arbitrary Galois number field by prime ideals of degree 1 and runs as follows.

Theorem 89. *In each ideal class of a Galois number field there exist ideals whose prime factors are all ideals of degree* 1.

We prove first the following Lemma.

Lemma 12. *Let K be a Galois number field of degree M and discriminant D; let $\mathfrak{P}$ be a prime ideal of K of degree f greater than 1 which does not divide $DM!$. Then there exists an integer Ω of K prime to $DM!$ which is divisible by $\mathfrak{P}$ but not by $\mathfrak{P}^2$ and whose remaining prime ideal factors are all of degree less than f.*

Proof. Let P be an integer of the field K such that every other integer Ω of K is congruent modulo $\mathfrak{P}^2$ to a polynomial in P with rational integer coefficients. (Such an integer P exists by Theorem 29.) We denote by $\mathfrak{P}'$, $\mathfrak{P}''$, $\ldots$, $\mathfrak{P}^{(m)}$ the prime ideals conjugate to $\mathfrak{P}$ and distinct from $\mathfrak{P}$ and determine an integer A of K which satisfies the congruences

$$\begin{aligned} \mathsf{A} &\equiv \mathsf{P} \pmod{\mathfrak{P}^2}, \\ \mathsf{A} &\equiv 0 \pmod{\mathfrak{P}'\mathfrak{P}''\cdots\mathfrak{P}^{(m)}}, \\ \mathsf{A} &\equiv 1 \pmod{M!}. \end{aligned}$$

If z is an automorphism in the decomposition group of $\mathfrak{P}$ for which we have

$z\mathsf{P} \equiv \mathsf{P}^p(\text{mod } \mathfrak{P})$ then obviously the f differences $\mathsf{A} - z\mathsf{A}$, $\mathsf{A} - z^2\mathsf{A}$, ..., $\mathsf{A} - z^{f-1}\mathsf{A}$ are prime to $\mathfrak{P}$. If s is an automorphism which does not belong to the decomposition group then $s\mathsf{A}$ is divisible by $\mathfrak{P}$ and consequently the difference $\mathsf{A} - s\mathsf{A}$ is prime to $\mathfrak{P}$. The different of A is thus prime to $\mathfrak{P}$ and hence it follows from the remark on p.6 that A is a generator of the field K. Referring to Theorem 31 we see that K is the inertia field of $\mathfrak{P}$ and hence A satisfies an equation of the form

$$\mathsf{A}^f + \alpha_1\mathsf{A}^{f-1} + \cdots + \alpha_f = 0,$$

where $\alpha_1, \ldots, \alpha_f$ are numbers in the decomposition field k of the prime ideal $\mathfrak{P}$. We denote by k', k'', ... the remaining subfields of K of the same degree M/f as k. Then A satisfies equations

$$\begin{aligned} \mathsf{A}^f + \alpha_1'\mathsf{A}^{f-1} + \cdots + \alpha_f' &= 0, \\ \mathsf{A}^f + \alpha_1''\mathsf{A}^{f-1} + \cdots + \alpha_f'' &= 0, \\ \ldots\ldots\ldots\ldots, \end{aligned}$$

where α_1', ..., α_f' are numbers in k', α_1'', ..., α_f'' numbers in k'' and so on. Next we determine f rational integers a_1, ..., a_f such that

$$a_1 \equiv \alpha_1, \ldots, a_f \equiv \alpha_f \quad (\text{mod } \mathfrak{P}).$$

This is possible since, according to Theorem 70, the ideal $\mathfrak{P}$ is of degree 1 in k. Next let b_1, ..., b_f be rational integers which satisfy the congruences

$$M!b_1 \equiv a_1, \ldots, M!b_f \equiv a_f \quad (\text{mod } p)$$

and for which none of the differences

$$\beta_1 = M!b_1 - \alpha_1, \beta_1' = M!b_1' - \alpha_1', \ldots$$

(with subscript 1) vanishes. We set

$$\mathsf{B} = \mathsf{A}^f + M!(b_1\mathsf{A}^{f-1} + b_2\mathsf{A}^{f-2} + \cdots + b_f).$$

Finally we denote by q_1, ..., q_l all the rational prime numbers distinct from p and greater than M which divide the discriminant A of A or the norms of the numbers β_1, β_1', ... If q_i is any one of these prime numbers then (since it can have at most M prime factors in K) at least one of the q_i ($> M$) numbers B, $\mathsf{B}+1$, $\mathsf{B}+2$, ..., $\mathsf{B}+q_i-1$ must be prime to q_i; say $\mathsf{B}+c_i$ is prime to q_i. Let now c be a rational integer which satisfies the l congruences $M!pc \equiv c_i$ (mod q_i) for $i = 1, 2, \ldots, l$; then we claim that

$$\Omega = \mathsf{B} + M!pc$$

is a number with the property described in Lemma 12.

To see this we notice first that according to the congruence $\mathsf{A} \equiv 1$ (mod $M!$) the number Ω is relatively prime to all rational primes less than

or equal to M; on the other hand, according to the definition of the number c, Ω is prime to all the prime numbers greater than M which divide A. Thus Ω is prime to all the prime numbers distinct from p which divide A.

Further, Ω is divisible by $\mathfrak{P}$ but not by $\mathfrak{P}'$, $\mathfrak{P}''$, ..., $\mathfrak{P}^{(m)}$ since $M!b_f \equiv a_f \not\equiv 0 \pmod{p}$. The number Ω can be represented in the form

$$\Omega = \mathsf{A}^f + m_1\mathsf{A}^{f-1} + \cdots + m_f,$$

where $m_1, \ldots, m_f$ are rational integers. Since $\mathsf{A} \equiv \mathsf{P} \pmod{\mathfrak{P}^2}$ and P can satisfy no polynomial congruence modulo $\mathfrak{P}^2$ of degree less than $2f$, it follows that Ω is not divisible by $\mathfrak{P}^2$.

Suppose Ω were divisible by a prime ideal $\mathfrak{Q}$ of degree f' greater than f. Let $1, z', (z')^2, \ldots, (z')^{f'-1}$ be f' automorphisms in the decomposition group of $\mathfrak{Q}$ which generate it along with its inertia group. Then we would have the f' congruences

$$\begin{aligned} \mathsf{A}^f + m_1\mathsf{A}^{f-1} + \cdots + m_f &\equiv 0 \pmod{\mathfrak{Q}}, \\ (z'\mathsf{A})^f + m_1(z'\mathsf{A})^{f-1} + \cdots + m_f &\equiv 0 \pmod{\mathfrak{Q}}, \\ \cdots\cdots\cdots \end{aligned}$$

This would imply that the discriminant A of the number A is divisible by $\mathfrak{Q}$, in contradiction to what was shown above.

Finally, suppose that Ω is divisible by a prime ideal $\mathfrak{Q}$ of degree f; then the decomposition field of $\mathfrak{Q}$ must be one of the fields k, k', k'', ... Suppose it is k'; then we may write

$$\Omega = \Omega - (\mathsf{A}^f + \alpha_1'\mathsf{A}^{f-1} + \cdots + \alpha_f') = \beta_1'\mathsf{A}^{f-1} + \cdots + \beta_f',$$

where $\beta_1', \ldots, \beta_f'$ are numbers in k'. Let $1, z', (z')^2, \ldots, (z')^{f-1}$ be f automorphisms in the decomposition group of $\mathfrak{Q}$ which generate it along with its inertia group. Then we would have

$$\begin{aligned} \beta_1'\mathsf{A}^{f-1} + \cdots + \beta_f' &\equiv 0 \pmod{\mathfrak{Q}}, \\ \beta_1'(z'\mathsf{A})^{f-1} + \cdots + \beta_f' &\equiv 0 \pmod{\mathfrak{Q}}, \\ \cdots\cdots\cdots \end{aligned}$$

from which it would follow that either A or β_1' is divisible by $\mathfrak{Q}$ which, according to what was said above, is not the case.

When we bear in mind that in every ideal class we can find an ideal which is prime to $DM!$ we see at once that Theorem 89 follows easily from Lemma 12. Theorem 89 was proved by Kummer for the case of cyclotomic fields (*Kummer* (6)).

15. Cyclic Extension Fields of Prime Degree

§54. Symbolic Powers. Theorem on Numbers with Relative Norm 1

We shall now derive a succession of fundamental theorems on abelian extension fields. In order to facilitate the statement and proof of these theorem we introduce some notation and conventions.

Let K be an algebraic number field of degree lm; suppose K is a cyclic extension of a field k of degree m and let the relative degree l of K over k be a prime number. Let the elements of the cyclic group of K over k be 1, S, $S^2, \ldots, S^{l-1}$. Then we define the notion of a *symbolic power* of a number A of K as follows: if A is any integer or fraction in the field K and $a, a_1, \ldots, a_{l-1}$ are any rational integers then the form

$$\mathsf{A}^a(S\mathsf{A})^{a_1}(S^2\mathsf{A})^{a_2}\cdots(S^{l-1}\mathsf{A})^{a_{l-1}}$$

will be abbreviated to

$$\mathsf{A}^{a+a_1S+a_2S^2+\cdots+a_{l-1}S^{l-1}} = \mathsf{A}^{F(S)},$$

where $F(S)$ is the integral polynomial in S appearing as the exponent of A on the left hand side. According to this from now on the symbolic $F(S)$-th power of A will always represent an integer or fraction in the field K. This symbolic exponentiation can be regarded as a generalisation of a notation introduced by Kronecker in the case of cyclotomic fields (*Kronecker* (1)).

We prove now in succession the following properties of the cyclic extension K over k.

Theorem 90. *Every integer or fraction* A *in* K *whose relative norm with respect to* k *is* 1 *is the symbolic* $(1-S)$*-th power of an integer* B *in* K.

Proof. Let x be a variable and Θ a generator of the field K. Then we set

$$\mathsf{A}_x = \frac{x+\Theta}{x+S\Theta}\mathsf{A} = (x+\Theta)^{1-S}\mathsf{A}$$

and

$$\mathsf{B}_x = 1 + \mathsf{A}_x^1 + \mathsf{A}_x^{1+S} + \mathsf{A}_x^{1+S+S^2} + \cdots + \mathsf{A}_x^{1+S+S^2+\cdots+S^{l-2}}.$$

When we recall that $A^{1+S+S^2+\cdots+S^{l-1}} = 1$ and hence also $A_x^{1+S+S^2+\cdots+S^{l-1}} = 1$ we see that $B_x^{1-S} = A_x$. Since B_x is a rational function of x which, as is easily seen, does not vanish identically in x, we may choose a rational integer $x = a$ such that B_a is a nonzero number in K. The number $B^* = B_a/(a+\Theta)$ satisfies the equation $A = (B^*)^{1-S}$. If we set $B^* = B/b$ where B is an algebraic integer in K and b is a rational integer, then we have also $A = B^{1-S}$.

§55. Fundamental Sets of Relative Units and Proof of Their Existence

A second important theorem about the field K concerns a property of the units in K. Suppose that among the m conjugate fields determined by k there are r_1 real fields and r_2 pairs of conjugate imaginary fields; according to Theorem 47 the number of units of k in a fundamental set is $r = r_1 + r_2 - 1$. We now define the concept of a *fundamental set of relative units* of the field K with respect to k. This is a set of $r+1$ units $H_1, \dots, H_{r+1}$ in the field K with the property that a unit of the form $H_1^{F_1(S)} \dots H_{r+1}^{F_{r+1}(S)}[\varepsilon]$ can be the $(1-S)$-th power of a unit in K only if the algebraic integers $F_1(\zeta), \dots, F_{r+1}(\zeta)$ are all divisible by $(1-\zeta)$. Here $F_1(S), \dots, F_{r+1}(S)$ are integer polynomials in S, $[\varepsilon]$ is either an arbitrary unit in k or a unit in K whose l-th power is a unit in k and ζ is an l-th root of unity such that $\zeta \neq 1$.

Theorem 91. *If the relative degree l of the cyclic extension K over k is an odd prime number then there exists in K a fundamental set of $r+1$ relative units, where r has the same meaning as in Theorem 47.*

Proof. Since $l \neq 2$ it follows that among the lm conjugate fields determined by K there are lr_1 real fields and lr_2 pairs of conjugate imaginary fields. Let $\varepsilon_1, \dots, \varepsilon_r$ be a fundamental set of units of the field k. Among the units of K choose a unit E_1 such that $E_1, \varepsilon_1, \dots, \varepsilon_r$ forms an independent set of units; then we shall show that the $r+l-1$ units $E_1, E_1^S, \dots, E_1^{S^{l-2}}, \varepsilon_1, \dots, \varepsilon_r$ must also be an independent set of units.

To prove this let us suppose to the contrary that $E_1^{F(S)} = \varepsilon^*$, where $F(S)$ is an integer polynomial of degree $l-2$ in S which does not vanish identically and ε^* is a unit of the field k. Since the polynomial $1 + S + \cdots + S^{l-1}$ is irreducible (see the remark at the end of Sect. 91) there must exist integer polynomials G_1, G_2 in S and a nonzero rational integer a such that

$$FG_1 + (1 + S + \cdots + S^{l-1})G_2 = a.$$

When we remark that

$$E_1^{1+S+\cdots+S^{l-1}} = \varepsilon^{**},$$

where ε^{**} is a unit in k, we deduce that $E_1^a = \varepsilon^{***}$, where ε^{***} is also a unit in k. This contradicts the choice of E_1.

Next we choose a unit E_2 such that E_2, E_1, E_1^S, ..., $\mathsf{E}_1^{S^{l-2}}$, ε_1, ..., ε_r is an independent set of units and prove in the same way as above that E_2, E_2^S, ..., $\mathsf{E}_2^{S^{l-2}}$, E_1, E_1^S, ..., $\mathsf{E}_1^{S^{l-2}}$, ε_1, ..., ε_r is an independent set of units. Proceeding in this way we produce a set of $r_1 + r_2 = r + 1$ units $\mathsf{E}_1, \ldots, \mathsf{E}_{r+1}$ such that

$$\mathsf{E}_i, \mathsf{E}_i^S, \ldots, \mathsf{E}_i^{S^{l-2}}, \varepsilon_1, \ldots, \varepsilon_r \quad (i = 1, 2, \ldots, r + 1)$$

form an independent set of units. The number of units in this set is

$$(r + 1)(l - 1) + r = lr_1 + lr_2 - 1.$$

Now let l^m be a power of l high enough that the expression

$$\mathsf{E}_1^{F_1(S)} \ldots \mathsf{E}_{r+1}^{F_{r+1}(S)}[\varepsilon], \tag{15.1}$$

in which $F_1(S), \ldots, F_{r+1}(S)$ are arbitrary integer polynomials of degree $(l-2)$ in S and $[\varepsilon]$ is as defined on p. 106, cannot be an l^m-th power of a unit in K unless all the coefficients of the $r + 1$ polynomials $F_1(S), \ldots, F_{r+1}(S)$ are divisible by l. That there must exist such a power l^m follows with the help of the $lr_1 + lr_2 - 1$ fundamental units of K which exist by Theorem 47.

Consider now the identity

$$(1 - S)^l = 1 - S^l + lG(S),$$

where G is an integer polynomial; according to this the $(1 - S)^{lm}$-th symbolic power of a number in K is also at the same time an actual l^m-th power. It follows that the expression (15.1) can be the $(1 - S)^{lm}$-th symbolic power of a unit only when the algebraic integers $F_1(\zeta)$, ..., $F_{r+1}(\zeta)$ are all divisible by $1 - \zeta$.

Let now e_1 be the largest non-negative rational integer such that an expression of the form (15.1) is a symbolic $(1 - S)^{e_1}$-th symbolic power of a unit without having all the numbers $F_1(\zeta)$, ..., $F_{r+1}(\zeta)$ divisible by $1 - \zeta$. Suppose we have

$$\mathsf{E}_1^{F_1(S)} \cdots \mathsf{E}_{r+1}^{F_{r+1}(S)}[\varepsilon] = \mathsf{H}_1^{(1-S)^{e_1}},$$

where $F_1(S), \ldots, F_{r+1}(S)$ are integer polynomials in S and $F_1(\zeta)$, say, is not divisible by $1 - \zeta$; $[\varepsilon]$ has the same meaning as before and H_1 is a unit in the field K. Next, let e_2 be the largest non-negative rational integer such that a corresponding expression formed from the units $\mathsf{E}_2, \ldots, \mathsf{E}_{r+1}$ is a $(1 - S)^{e_2}$-th symbolic power of a unit, say

$$\mathsf{E}_2^{F_2(S)} \cdots \mathsf{E}_{r+1}^{F_{r+1}(S)}[\varepsilon] = \mathsf{H}_2^{(1-S)^{e_2}},$$

where $F_2(S), \ldots, F_{r+1}(S)$ are again integer polynomials in S and $F_2(\zeta)$, say, is not divisible by $1 - \zeta$; H_2 is a unit in K. Proceeding in this way we produce $r + 1$ units H_1, ..., H_{r+1}. We claim that these form a fundamental set of relative units of K with respect to k.

To prove this, let us suppose to the contrary that there are $r+1$ polynomials $G_1(S), \ldots, G_{r+1}(S)$ such that

$$\mathsf{H}_1^{G_1(S)} \cdots \mathsf{H}_{r+1}^{G_{r+1}(S)}[\varepsilon] = \mathsf{Z}^{1-S}$$

where Z is a unit in K and $G_1(\zeta), \ldots, G_{r+1}(\zeta)$ are not all divisible by $1-\zeta$. Let $G_h(\zeta)$ be the first of these numbers which is not divisible by $1-\zeta$; then clearly the factor

$$\mathsf{H}_h^{G_h(S)}\mathsf{H}_{h+1}^{G_{h+1}(S)} \cdots \mathsf{H}_{r+1}^{G_{r+1}(S)}[\varepsilon]$$

must also be the $(1-S)$-th symbolic power of a unit in K. Since none of the integers $e_1, e_2, \ldots, e_{r+1}$ is greater than any of those which precede it we see that when we raise the last expression to the $(1-S)^{e_h}$-th power and introduce again the units $\mathsf{E}_h, \ldots, \mathsf{E}_{r+1}$ we reach a contradiction.

It is easily seen that Theorem 91 holds also for $l=2$ provided that in this case we have the additional condition that among the $2m$ conjugate fields determined by K there are twice as many real fields as there are among the m conjugate fields determined by k.

§56. Existence of a Unit in K with Relative Norm 1 Which is not the Quotient of Two Relatively Conjugate Units

Theorem 92. *If the relative degree of the cyclic extension K over k is an odd prime number l then there exists a unit H in K whose relative norm with respect to k is 1 but which is not the symbolic $(1-S)$-th power of a unit in K.*

Proof. We suppose first that the field K does not contain the l-th root of unity ζ. Let $\eta_1, \ldots, \eta_{r+1}$ be any $r+1$ units in k; then it follows that there are $r+1$ rational integers $a_1, \ldots, a_{r+1}$, not all divisible by l, such that $\eta_1^{a_1} \cdots \eta_{r+1}^{a_{r+1}} = 1$. (If in an equation of this form the exponents $a_1, \ldots, a_{r+1}$ were all divisible by l then $\eta_1^{a_1/l} \cdots \eta_{r+1}^{a_{r+1}/l}$ would be an l-th root of unity and hence, by hypothesis, equal to 1. Repetition of this argument establishes the assertion.) Now let us suppose that $\eta_1, \ldots, \eta_{r+1}$ are the relative norms of $\mathsf{H}_1, \ldots, \mathsf{H}_{r+1}$, where $\mathsf{H}_1, \ldots, \mathsf{H}_{r+1}$ form a fundamental set of relative units of K with respect to k. Set $\mathsf{H} = \mathsf{H}_1^{a_1} \cdots \mathsf{H}_{r+1}^{a_{r+1}}$; then $N_k(\mathsf{H}) = \mathsf{H}^{1+S+S^2+\cdots+S^{l-1}} = 1$ and hence, by Theorem 90, there is an integer A of K such that $\mathsf{H} = \mathsf{A}^{1-S}$. Since $\mathsf{H}_1, \ldots, \mathsf{H}_{r+1}$ make up a fundamental set of relative units it follows that A is not a unit.

To complete the proof of Theorem 92 let us suppose that k contains a primitive l^h-th root of unity ζ' but no primitive l^{h+1}-th root of unity. By an argument similar to that used above we can show that if $\eta_1, \ldots, \eta_{r+2}$ are

any $r+2$ units in k there exist a rational integer a and $r+2$ rational integers $a_1, \ldots, a_{r+2}$, not all divisible by l, such that

$$\eta_1^{a_1} \cdots \eta_{r+2}^{a_{r+2}} = (\zeta')^{al}.$$

On the other hand, since the relative norm

$$N_k(\zeta) = \zeta^{1+S+S^2+\cdots+S^{l-1}} = 1,$$

it follows from Theorem 90 that ζ must be a symbolic $(1-S)$-th power. If there were no unit E in K such that $\zeta = \mathsf{E}^{1-S}$ then ζ would be already a number with the desired property. Otherwise we have $\mathsf{E}^{l(1-S)} = 1$, i.e. $\mathsf{E}^l = S\mathsf{E}^l$, so that E^l is a unit ε in k, while E itself certainly does not lie in k. We have $N_k(\mathsf{E}) = \mathsf{E}^l = \varepsilon$. Now let $\mathsf{H}_1, \ldots, \mathsf{H}_{r+1}$ be a fundamental set of relative units in K and set

$$\eta_1 = N_k(\mathsf{H}_1), \ldots, \eta_{r+1} = N_k(\mathsf{H}_{r+1}), \eta_{r+2} = N_k(\mathsf{E}) = \mathsf{E}^l,$$

$$\mathsf{H} = \mathsf{H}_1^{a_1} \cdots \mathsf{H}_{r+1}^{a_{r+1}} \mathsf{E}^{a_{r+2}} (\zeta')^{-a} = \mathsf{H}_1^{a_1} \cdots \mathsf{H}_{r+1}^{a_{r+1}} [\varepsilon],$$

where $a, a_1, \ldots, a_{r+2}$ are the numbers described above and $[\varepsilon]$ is the l-th root of a unit of the field k. Then $N_k(\mathsf{H}) = 1$. The numbers $a_1, \ldots, a_{r+1}$ cannot all be divisible by l, for, if they were, it would follow from the equation

$$(\eta_1^{a_1/l} \cdots \eta_{r+1}{}^{a_{r+1}/l} \mathsf{E}^{a_{r+2}} (\zeta')^{-a})^l = 1$$

that

$$\eta_1^{a_1/l} \cdots \eta_{r+1}{}^{a_{r+1}/l} \mathsf{E}^{a_{r+2}} (\zeta')^{-a} = \zeta^b,$$

where b is a rational integer. Since, by hypothesis, a_{r+2} cannot also be divisible by l it would follow from the last equation that E lies in k, which is not the case. Thus the unit H fulfils the conditions of Theorem 92.

Theorems 90, 91 and 92 were already proved in part and in another form by Kummer in the case where the subfield k is the cyclotomic field of degree $l-1$ generated by ζ (*Kummer* (14, 20, 21)).

§57. Ambig Ideals and the Relative Different of a Cyclic Extension

An ideal $\mathfrak{A}$ of a cyclic extension field K of k is called an *ambig ideal*[1] if it is invariant under the automorphism S and has no ideal of k as a factor. In

[1] We follow the example of Artin in his lectures in leaving *ambig* untranslated: the obvious translation *ambiguous* does not catch the sense.

particular a prime ideal of K which is invariant under S and does not lie in k is called an *ambig prime ideal*

Theorem 93. *If K is a cyclic extension of k, then the relative different of K with respect to k is divisible by the ambig prime ideals $\mathfrak{P}$ and by no others.*

Proof. Let $\mathfrak{P}$ be an ambig prime ideal; its relative norm $N_k(\mathfrak{P})$ is $\mathfrak{P}^l$. Since no lower power of $\mathfrak{P}$ can lie in k it follows that $\mathfrak{P}^l = \mathfrak{p}$ is a prime ideal in k. Conversely, when a prime ideal $\mathfrak{p}$ of k is equal to the l-th power of an ideal $\mathfrak{P}$ in K then $\mathfrak{P}$ must be an ambig prime ideal.

We now distinguish three types of prime ideals $\mathfrak{p}$ of the field k: (1) those which are equal to the l-th power of a prime ideal $\mathfrak{P}$ in K: (2) those which split in K as a product of l distinct prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_l$ of K; (3) those which are also prime ideals in K.

In case (1) we suppose that the norm $N(\mathfrak{P})$ is p^f; it follows that $N(\mathfrak{p}) = N(\mathfrak{P}^l) = p^{lf}$ and hence the norm $n(\mathfrak{p})$ of the prime ideal $\mathfrak{p}$ in k is also p^f. The fact that the norms $N(\mathfrak{P})$ and $n(\mathfrak{p})$ are equal shows that every integer of K is congruent modulo $\mathfrak{P}$ to some integer of k; from this we deduce easily that the relative different of K with respect to k must be divisible by the prime ideal $\mathfrak{P}$.

In case (2) we can find an integer A which is not divisible by $\mathfrak{P}_i$ but is divisible by the remaining $l-1$ prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_{i-1}, \mathfrak{P}_{i+1}, \ldots, \mathfrak{P}_l$. From this it follows that the relative different of the number A and hence also that of the field K is not divisible by $\mathfrak{P}_i$.

Finally, in case (3), let P be a primitive root for the prime ideal $\mathfrak{p}$ in k and ρ a primitive root for $\mathfrak{p}$ in k; suppose P is also a generator of the field K. Then P satisfies an equation of degree l of the form

$$F(\mathsf{P}) = \mathsf{P}^l + \alpha_1 \mathsf{P}^{l-1} + \cdots + \alpha_l = 0,$$

with coefficients $\alpha_1, \ldots, \alpha_l$ which are integers in k. We set

$$\alpha_1 \equiv f_1(\rho), \ldots, \alpha_l \equiv f_l(\rho) \pmod{\mathfrak{p}}$$

where $f_1(\rho), \ldots, f_l(\rho)$ are integer polynomials in ρ; thus we obtain for P the congruence

$$F(\mathsf{P}) \equiv \mathsf{P}^l + f_1(\rho)\mathsf{P}^{l-1} + \cdots + f_l(\rho) \equiv 0 \pmod{\mathfrak{p}}.$$

Since $N(\mathfrak{p}) = (n(\mathfrak{p}))^l$ the number of integers of K incongruent modulo $\mathfrak{p}$ is the l-th power of the number of integers of k incongruent modulo $\mathfrak{p}$; it follows that P can satisfy no congruence of this type of degree less than l and hence we have

$$\frac{\partial F(\mathsf{P})}{\partial \mathsf{P}} \not\equiv 0 \pmod{\mathfrak{p}}.$$

Thus the relative different of the number P is not divisible by $\mathfrak{p}$.

This discussion shows that the relative different of the field K is always prime to the prime ideals of types (2) and (3) and so completes the proof of Theorem 93.

§58. Fundamental Theorem on Cyclic Extensions with Relative Different 1. Designation of These Fields as Class Fields

Theorems 90, 92 and 93 make it possible for us to establish a fact which is of far-reaching importance in the theory of algebraic number fields. This result is as follows.

Theorem 94. *If the cyclic extension field K of odd prime degree l over k has relative different 1 with respect to k then there exists an ideal $\mathfrak{i}$ in k which is not a principal ideal in k but which is a principal ideal in K. The l-th power of this ideal $\mathfrak{i}$ is then necessarily a principal ideal in the field k and hence the class number of k is divisible by l.*

Proof. By Theorem 92 there is a unit H of K with relative norm 1 which is not the $(1-S)$-th power of a unit. According to Theorem 90 we have $\mathsf{H} = \mathsf{A}^{1-S}$ where A is an integer in K, i.e. $\mathsf{A} = \mathsf{H} \cdot S\mathsf{A}$. For the principal ideal $\mathfrak{A} = (\mathsf{A})$ it follows from this that $\mathfrak{A} = S\mathfrak{A}$. The ideal $\mathfrak{A}$ lies in the field k. For if $\mathfrak{P}$ is any prime ideal of K which divides $\mathfrak{A}$ and does not lie in k then, according to Theorem 93 (since by hypothesis the relative different has no divisors) we have $\mathfrak{P} \neq S\mathfrak{P}$ and so $\mathfrak{A}$ includes also the relative norm $N_k(\mathfrak{P})$ which is a prime ideal in k. The ideal $\mathfrak{A}$ is not a principal ideal in the field k; for, if it were, we would have $\mathsf{A} = \mathsf{H}^*\alpha$ where H^* is a unit and α is a number in k; from this it would follow that $\mathsf{H} = (\mathsf{H}^*)^{1-S}$, which contradicts the definition of H. This establishes the first part of Theorem 94.

Since $N_k(\mathsf{A}) = \alpha$ is a number in k and consequently $N_k(\mathfrak{A}) = \mathfrak{A}^l = (\alpha)$ is a principal ideal in k, this completes the proof of Theorem 94.

Theorems 92 and 94 hold for the case where $l = 2$ under the restrictions mentioned on p. 108 at the end of Sect. 55.

There is no essential difficulty in generalising Theorem 94 to abelian extension fields K with relative different 1 where the relative degree l is not a prime number.

On account of the close connexion shown by Theorem 94 between the field K and certain ideal classes of k, we call K a *class field* of the field k.

Part III

Quadratic Number Fields

16. Factorisation of Numbers in Quadratic Fields

§59. Basis and Discriminant of a Quadratic Field

Let $m \neq 1$ be a positive or negative rational integer which is not divisible by any square number other than 1; the quadratic equation

$$x^2 - m = 0$$

is then irreducible over the field of rational numbers. In the following, when m is positive we shall take $\sqrt{m}$ to be the positive root of the equation and when m is negative $\sqrt{m}$ will be the positive imaginary root of the equation. The algebraic number $\sqrt{m}$ so determined generates a real or imaginary quadratic field according as m is positive or negative. We denote this field by $k(\sqrt{m})$ or simply by k; it is always a Galois number field. Under the operation of interchanging $\sqrt{m}$ with $-\sqrt{m}$ a number or an ideal of the field k is transformed into its conjugate number or ideal respectively. This operation (which is an automorphism of k) will be denoted by s.

Our first task is to find a basis for each quadratic field and to determine its discriminant (*Dedekind* (1)).

Theorem 95. *A basis for the quadratic field k is formed by the numbers* 1 *and ω where*

$$\omega = \frac{1+\sqrt{m}}{2} \quad \text{or} \quad \omega = \sqrt{m}$$

according as m is congruent to 1 *modulo* 4 *or not. The discriminant of k is*

$$d = m \quad \text{or} \quad d = 4m$$

in these two cases respectively.

Proof. The number ω is an integer since it satisfies the equation

$$x^2 - x - \frac{m-1}{4} = 0 \;\; \text{or} \;\; x^2 - m = 0 \qquad (16.1)$$

respectively. Let $\omega' = s\omega$ be the conjugate of ω. Then $d = (\omega - \omega')^2$ is the discriminant of the number ω. According to Sect. 3, p. 6, every integer of the field k can be represented in the form

$$\alpha = \frac{u + v\omega}{d}$$

where u and v are rational integers.

In the case where $m \equiv 1 \pmod 4$ we conclude from the congruence

$$2\alpha m = 2u + v + v\sqrt{m} \equiv 0 \pmod m$$

that $2u + v$ must be divisible by $\sqrt{m}$. This leads to the result that $v\sqrt{m} \equiv 0 \pmod m$; thus v must be divisible by $\sqrt{m}$ and hence by m. It follows that u and v are both divisible by $m = d$; so the integer d in the denominator of the above fraction can be cancelled.

On the other hand, when $m \not\equiv 1 \pmod 4$ we conclude from the congruence

$$4\alpha m = u + v\sqrt{m} \equiv 0 \pmod m$$

that u and v must be divisible by m and hence m can be cancelled from the numerator and denominator of the representation of α. So we obtain

$$\alpha = \frac{u' + v'\sqrt{m}}{4}$$

where u' and v' are rational integers. In the case where $m \equiv 2 \pmod 4$ and also where $m \equiv 3 \pmod 4$ we can easily see by considering the norm $\alpha \cdot s\alpha$ that an expression of the form $u' + v'\sqrt{m}$ (where u' and v' are rational integers) can be divisible by 2 only if u' and v' are both even. Applying this observation to 4α and again to 2α we see that in the case where $m \not\equiv 1 \pmod 4$ every integer in the field k can be expressed in the form $u + v\sqrt{m}$ where u and v are rational integers.

The second part of the theorem follows from the formula

$$d = \begin{vmatrix} 1 & \omega \\ 1 & \omega' \end{vmatrix}^2 = (\omega - \omega')^2$$

which, according to Sect. 3, defines the discriminant of the field.

§60. Prime Ideals of a Quadratic Field

The problem of describing the factorisation of a rational prime number into prime ideals of the field k is completely settled by the following theorem.

Theorem 96. *Every rational prime number l which divides d is equal to the square of a prime ideal in k. Every odd rational prime number p which does not divide d either splits in k as a product of two distinct prime ideals $\mathfrak{p}$ and $\mathfrak{p}'$ of degree 1 and conjugate to one another or else represents a prime ideal of degree 2 in k according as d is a quadratic residue or non-residue*

modulo p. In the case where $m \equiv 1 \pmod 4$ the prime number 2 either splits in k as a product of two distinct conjugate prime ideals or else remains prime according as $m \equiv 1 \pmod 8$ or $m \equiv 5 \pmod 8$.

Proof. The first assertion of the theorem, concerning the prime numbers l which divide d, is a consequence of the general Theorem 31. If l is an odd prime dividing d we find

$$l = \mathfrak{l}^2$$

where $\mathfrak{l} = (l, \sqrt{m})$ is a prime ideal of degree 1 which coincides with its conjugate. If the prime number 2 divides d then we have

$$2 = (2, \sqrt{m})^2 \quad \text{or} \quad 2 = (2, 1 + \sqrt{m})^2$$

according as $m \equiv 2 \pmod 4$ or $m \equiv 3 \pmod 4$.

The factorisation of the prime numbers which do not divide d occurs according to Theorem 33 when we take account of the remark referring to it in Sect. 13, p. 31. Thus every rational prime number p which is prime to d either splits in k as a product of two distinct prime ideals or else is itself a prime ideal according as the left hand side of the equations (16.1) are reducible or irreducible modulo p. If the prime number p under consideration is odd then the congruences

$$(2x - 1)^2 - m \equiv 0 \pmod p \quad \text{and} \quad x^2 - m \equiv 0 \pmod p$$

respectively are reducible when m is a quadratic residue modulo p and irreducible when m is a quadratic non-residue modulo p. If, in the first case, we have $m \equiv a^2 \pmod p$ then

$$p = (p, a + \sqrt{m})(p, a - \sqrt{m}) = \mathfrak{p}\mathfrak{p}'.$$

Since

$$(p, a + \sqrt{m}, a - \sqrt{m}) = 1$$

the prime ideals $\mathfrak{p}$ and $\mathfrak{p}'$ on the right hand side are in fact distinct. In the case where $m \equiv 1 \pmod 4$ the congruence

$$x^2 - x - \frac{m-1}{4} \equiv 0 \pmod 2$$

is obviously reducible or irreducible according as $\frac{m-1}{4}$ is congruent to 0 or 1 modulo 2, i.e. according as $m \equiv 1$ or $m \equiv 5 \pmod 8$. In the first case we have

$$2 = \left(2, \frac{1+\sqrt{m}}{2}\right)\left(2, \frac{1-\sqrt{m}}{2}\right).$$

Since

$$\left(2, \frac{1+\sqrt{m}}{2}, \frac{1-\sqrt{m}}{2}\right) = 1$$

the two prime ideals on the right hand side are in fact distinct.

As bases for the prime ideals introduced above we may take

$$\begin{array}{lcl} l, \dfrac{l+\sqrt{m}}{2} & \text{or} & l, \sqrt{m}, \\ p, \dfrac{a \pm \sqrt{m}}{2} & \text{or} & p, a \pm \sqrt{m}, \\ 2, \dfrac{1 \pm \sqrt{m}}{2} & \text{or} & 2, \sqrt{m}; 2, 1+\sqrt{m} \end{array}$$

according as $m \equiv 1 \pmod 4$ or $m \equiv 2$ or $3 \pmod 4$. These facts are easily verified by applying a converse of Theorem 19 if in each case we form the determinant of the given pair of numbers and their conjugates. (In the second row of the above table a is an integer satisfying the congruence $a^2 \equiv m \pmod p$; if $m \equiv 1 \pmod 4$ then a is to be an odd number.)

§61. The Symbol $\left(\dfrac{a}{w}\right)$

To enable us to express more concisely the results we have obtained about the factorisation of rational prime numbers we introduce the following symbol. Let a be any rational integer. If w is an odd rational prime number then the symbol $\left(\frac{a}{w}\right) = +1$ if a is a quadratic residue modulo w not divisible by w; $\left(\frac{a}{w}\right) = -1$ if a is a quadratic non-residue modulo w; and $\left(\frac{a}{w}\right) = 0$ if a is divisible by w. Further $\left(\frac{a}{2}\right) = +1$ if a is odd and a quadratic residue modulo 8; $\left(\frac{a}{2}\right) = -1$ if a is odd and a quadratic non-residue modulo 8; and $\left(\frac{a}{2}\right) = 0$ if a is even. When we use these symbols Theorem 96 assumes the following form.

Theorem 97. *A rational prime number p (odd or even) is the product of two distinct prime ideals of k or generates a prime ideal of k or is the square of a prime ideal in k according as $\left(\frac{d}{p}\right) = +1$, -1 or 0 respectively (Dedekind* (1)).

According to the results we have developed so far we distinguish three types of prime ideals, namely

1. the prime ideals $\mathfrak{p}$ of degree 1 which are distinct from their conjugates $\mathfrak{p}'$;

2. the prime ideals (p) of degree 2 which are represented by the rational prime numbers p which do not split in k;

3. the prime ideals $\mathfrak{l}$ of degree 1 whose squares are rational prime numbers dividing d.

According to the definitions introduced in Sect. 39 and Sect. 41 the field k is the decomposition field for the prime ideals $\mathfrak{p}$ of the first type, the inertia field for the prime ideals (p) of the second type and the ramification field for the prime ideals $\mathfrak{l}$ of the third type.

§62. Units of a Quadratic Field

When we consider the subject of units in a quadratic field k we see from Theorem 47 that we must distinguish two cases depending on whether k is an imaginary or a real field.

In the first case k contains no units other than roots of unity. Since the only roots of unity apart from $+1$ and -1 which can occur in a quadratic field are the 3rd, 4th and 6th roots of unity it follows that the only imaginary quadratic fields which contain roots of unity other than $+1$ and -1 are the two fields $k(\sqrt{-1})$ and $k(\sqrt{-3})$. The first of these contains the two units $\pm i$, the second the four units $\pm\dfrac{1\pm\sqrt{-3}}{2}$. The discriminants of these two fields are respectively -4 and -3; according to Theorem 50 each ideal class of these fields must contain an ideal with norm ≤ 2 or $\leq |\sqrt{3}|$ respectively. Further, since in the field $k(\sqrt{-1})$ the number 2 is the norm of the principal ideal $(1+i)$, it follows that each of these two quadratic fields has only *one* ideal class. Thus in each of these two fields there are only principal ideals and consequently every positive rational integer which is the norm of an ideal in $k(\sqrt{-1})$ or $k(\sqrt{-3})$ must be the norm of an algebraic integer in the corresponding field; from this we deduce the well-known results on the representation of positive rational integers in the forms x^2+y^2, x^2+xy+y^2 respectively where x and y are rational integers.

If on the other hand k is a real quadratic field it follows from Theorem 47 that there exists a fundamental unit ε, distinct from ± 1, such that every unit in the field can be expressed uniquely in the form $\pm\varepsilon^a$ where a is a rational integer.

The conditions under which the norm of this fundamental unit ε is equal to $+1$ or -1 have so far been determined only in particular cases (*Arndt* (1), *Dirichlet* (4), *Legendre* (1), *Tano* (1)). (See also on page 127 the first part of the proof of Lemma 13.)

§63. Composition of the Set of Ideal Classes

The discussion in Sect. 24 makes it possible for each particular value of m to list all the ideal classes of the quadratic field k and to calculate the number h of these classes. Hitherto tables of such results have been prepared on the basis of the theory of reduced quadratic forms (*Gauss* (1), *Cayley* (1)).

17. Genera in Quadratic Fields and Their Character Sets

§64. The Symbol $\left(\frac{n,m}{w}\right)$

For the further development of the theory of quadratic fields, particularly in order to classify the ideal classes of such a field, we make use of a new symbol. Let n and m be rational integers, with m not the square of an integer; let w be any rational prime number. Then the symbol $\left(\frac{n,m}{w}\right)$ takes the value $+1$ whenever n is congruent modulo w to the norm of an integer of the quadratic field $k(\sqrt{m})$ determined by $\sqrt{m}$ and in addition for each higher power of w there exists an integer in $k(\sqrt{m})$ whose norm is congruent to n modulo the corresponding power of w; in every other situation we set $\left(\frac{n,m}{w}\right) = -1$. The rational integers n for which $\left(\frac{n,m}{w}\right) = +1$ are called *norm residues* of the field $k(\sqrt{m})$ modulo w; the integers n for which $\left(\frac{n,m}{w}\right) = -1$ are called *norm non-residues* of $k(\sqrt{m})$ modulo w. If m is the square of an integer we shall always take $\left(\frac{n,m}{w}\right)$ to be $+1$. The following theorem gives us information concerning the properties of the symbol $\left(\frac{n,m}{w}\right)$ which are useful in calculations.

Theorem 98. *Let n and m be rational integers not divisible by w. Then we have the following rules. If w is an odd prime number then*

$$\left(\frac{n,m}{w}\right) = +1, \tag{17.1}$$

$$\left(\frac{n,w}{w}\right) = \left(\frac{w,n}{w}\right) = \left(\frac{n}{w}\right). \tag{17.2}$$

If $w = 2$ then

$$\left(\frac{n,m}{2}\right) = (-1)^{(n-1)(m-1)/4}, \tag{17.3}$$

$$\left(\frac{n,2}{2}\right) = \left(\frac{2,n}{2}\right) = (-1)^{(n^2-1)/8}. \tag{17.4}$$

Furthermore for all rational integers n, n', m, m' and all prime numbers w we have

$$\left(\frac{-m, m}{w}\right) = +1, \tag{17.5}$$

$$\left(\frac{n, m}{w}\right) = \left(\frac{m, n}{w}\right), \tag{17.6}$$

$$\left(\frac{nn', m}{w}\right) = \left(\frac{n, m}{w}\right)\left(\frac{n', m}{w}\right), \tag{17.7}$$

$$\left(\frac{n, mm'}{w}\right) = \left(\frac{n, m}{w}\right)\left(\frac{n, m'}{w}\right). \tag{17.8}$$

Proof. We begin with the self-evident remark that if n is itself the norm of an integer in the field $k(\sqrt{m})$ then we have $\left(\frac{n, m}{w}\right) = +1$. Since, in particular, $-m$ is the norm of $\sqrt{m}$, equation (17.5) follows at once. If n and n' are nonzero rational integers whose quotient is the norm of an integer or fraction in $k(\sqrt{m})$ then it follows from the definition of the symbols that $\left(\frac{n, m}{w}\right) = \left(\frac{n', m}{w}\right)$. This is the case, in particular, when the quotient n/n' is the square of a rational number; so we obtain the simple result that the value of the symbol $\left(\frac{n, m}{w}\right)$ remains unaltered when n is multiplied by a square or has a square factor removed from it. For the sake of simplicity we shall assume from now on that neither n nor m is divisible by the square of a prime number.

To establish the complete set of formulæ we deal in turn with the following three cases.

1. Let w be an odd prime number which divides m.

If n is not divisible by w then clearly the congruences

$$4n \equiv (2x+y)^2 - my^2 \text{ and } n \equiv x^2 - my^2 \pmod{w} \tag{17.9}$$

are solvable in rational integers x and y if and only if $\left(\frac{n}{w}\right) = +1$. Conversely, if this condition is satisfied, the congruence $n \equiv x^2$ is solvable modulo each power of w and hence the same holds for the congruences (17.9). Under the hypotheses we have made it follows that

$$\left(\frac{n, m}{w}\right) = \left(\frac{n}{w}\right).$$

On the other hand, if n also is divisible by w we have

$$\left(\frac{n, m}{w}\right) = \left(\frac{-nm, m}{w}\right) = \left(\frac{-nm/w^2, m}{w}\right) = \left(\frac{-nm/w^2}{w}\right).$$

2. Next let w be an odd prime number which does not divide m.

If n also is not divisible by w then we claim that the congruence $n \equiv x^2 - my^2 \pmod{w}$ always has solutions. For the right hand side of this congruence gives for $x = 1, 2, \ldots, \frac{1}{2}(w-1)$ and $y = 0$ all the quadratic residues modulo w. In the case where $\left(\frac{-m}{w}\right) = -1$ it gives for $x = 0$ and $y = 1, 2, \ldots, \frac{1}{2}(w-1)$ all the quadratic non-residues modulo w. If $\left(\frac{-m}{w}\right) = +1$ we let a be the least positive quadratic non-residue modulo w and take $y = b$ to be a root of the (clearly solvable) congruence $-my^2 \equiv a - 1 \pmod{w}$; since $a \equiv 1 - mb^2$ modulo w the form $x^2 - m(bx)^2$ for $x = 1, 2, \ldots, \frac{1}{2}(w-1)$ represents all the quadratic non-residues modulo w. From the fact that the congruence $n \equiv x^2 - my^2 \pmod{w}$ is solvable it follows easily that the congruence is solvable modulo every power of w. Thus, under the current hypotheses, we have

$$\left(\frac{n,m}{w}\right) = +1.$$

If, on the other hand, n is divisible by w (but, by our original agreement, not by w^2) a solution of the congruence $n \equiv x^2 - my^2 \pmod{w^2}$ would give rise to an integer $\alpha = x - \sqrt{m}y$ of the field $k(\sqrt{m})$ for which the norm $\alpha \cdot s(\alpha) = n(\alpha)$ contains only w but not w^2 as a factor; it follows that w would split in the field $k(\sqrt{m})$ as a product of two distinct prime ideals $\mathfrak{w}$ and $\mathfrak{w}'$; according to Theorem 97 the necessary condition for this is that $\left(\frac{m}{w}\right) = +1$. Conversely, when this condition is satisfied, w splits in the field $k(\sqrt{m})$ as a product $\mathfrak{w}\mathfrak{w}'$ of two distinct prime ideals. Then let α be an integer in $k(\sqrt{m})$ which is divisible by w but not by $\mathfrak{w}'$ nor $\mathfrak{w}^2$; it follows that

$$\left(\frac{n,m}{w}\right) = \left(\frac{n \cdot n(\alpha), m}{w}\right) = \left(\frac{n \cdot n(\alpha)/w^2, m}{w}\right) = +1.$$

Thus we have shown that under the current conditions we always have $\left(\frac{n,m}{w}\right) = \left(\frac{m}{w}\right)$.

The results we have obtained so far allow us to deduce immediately the formulæ (17.1) and (17.2); furthermore, we deduce formulæ (17.6) and (17.7) for odd primes w if we consider successively the different cases of divisibility and non-divisibility by w of n, n' and m.

3. For the case where $w = 2$ we begin by making the following assertion: if $f(x, y)$ is an integer polynomial, homogeneous of degree 2 in x and y, and n is an odd rational integer then, if the congruence $f(x, y) \equiv n \pmod{2^3}$ has rational integer solutions for x and y then so also do all the congruences $f(x, y) \equiv n \pmod{2^{e+1}}$ for all $e \geq 3$. We prove this by induction on e. So suppose that a and b are rational integers for which $n \equiv f(a, b) \pmod{2^e}$, where the exponent $e \geq 3$. If we do not also have $n \equiv f(a, b) \pmod{2^{e+1}}$ but

rather $n \equiv f(a,b) + 2^e \pmod{2^{e+1}}$ then we determine a rational integer c such that $c^2 \equiv 1 + 2^e \pmod{2^{e+1}}$ (which is possible since $e \geq 3$). Then we have

$$f(ca, cb) = c^2 f(a,b) \equiv f(a,b) + 2^e f(a,b) \equiv f(a,b) + 2^e \equiv n \pmod{2^{e+1}}$$

and so our assertion is proved.

To determine the value of the symbol $\left(\frac{m,n}{2}\right)$ for an odd integer n we have to investigate for which combinations of values of n and m the congruences

$$n \equiv x^2 + xy - \frac{m-1}{4} y^2 \pmod{2^3} \tag{17.10}$$

(in the case where $m \equiv 1 \pmod 4$) and

$$n \equiv x^2 - my^2 \pmod{2^3} \tag{17.11}$$

(when $m \equiv 2$ or $3 \pmod 4$) are solvable. Brief calculations lead to the following table, in which we list under the heading m the six residues of m modulo 2^3 with which we are concerned and under the heading n the odd residues modulo 2^3 for which the corresponding congruences (17.10) and (17.11) are solvable.

m	n
1	1, 3, 5, 7
2	1, 7
3	1, 5
5	1, 3, 5, 7
6	1, 3
7	1, 5

This table establishes formula (17.3) in the case where n and m are both odd; in the case where n is odd and m is even, say $m = 2m'$, we deduce from the table that

$$\left(\frac{n, 2m'}{2}\right) = (-1)^{(n^2-1)/8 + (n-1)(m'-1)/4}.$$

On the other hand, if n is even, say $n = 2n'$, and m is odd, then we have to distinguish the cases where $m \equiv 1$ and $m \equiv 3$ modulo 4. In the first case the number 2 must be the product of two distinct prime ideals in the field $k(\sqrt{m})$ if $n = 2n'$ is a norm residue modulo 2 in $k(\sqrt{m})$, i.e. $\left(\frac{m}{2}\right) = +1$. If this condition is satisfied we can always find a number α in $k(\sqrt{m})$ for which the norm $n(\alpha)$ is divisible by 2 and not by 4. It follows that

$$\left(\frac{2n', m}{2}\right) = \left(\frac{2n' \cdot n(\alpha), m}{2}\right) = \left(\frac{\frac{n' \cdot n(\alpha)}{2}, m}{2}\right),$$

and according to (17.3) this last symbol is equal to +1; hence in this case we have the formula

$$\left(\frac{2n', m}{2}\right) = \left(\frac{m}{2}\right) = (-1)^{(m^2-1)/8}.$$

In the other case, where $m \equiv 3$ modulo 4, the value of the symbol in question depends on the solvability of the congruence $2n' \equiv x^2 - my^2$ modulo arbitrarily high powers 2^e and it is easy to see that each such congruence is solvable if and only if the congruence $m \equiv x^2 - 2n'y^2$ is solvable modulo the same power 2^e. Thus in this case we have

$$\left(\frac{2n', m}{2}\right) = \left(\frac{m, 2n'}{2}\right).$$

Finally, suppose n and m are both even, say $n = 2n'$ and $m = 2m'$. Then we have

$$\left(\frac{2n', 2m'}{2}\right) = \left(\frac{-2^2n'm', 2m'}{2}\right) = \left(\frac{-n'm', 2m'}{2}\right).$$

From the results we have obtained we deduce formula (17.4) at once; at the same time we see that formulæ (17.6) and (17.7) are valid also for $w = 2$. Formula (17.8) follows in general by combining (17.7) with (17.6). Thus the proof of Theorem 98 is complete.

From the formulæ (17.1), (17.2), (17.3) and (17.4) in Theorem 98 we may deduce the following result.

Consider a complete set of numbers prime to w and incongruent modulo w^e, where $e \geq 1$ (in the case where $w = 2$ we take $e > 2$). Then either all the numbers in the set are norm residues of the quadratic field $k(\sqrt{m})$ modulo w or else only half of them, according as w is prime to the discriminant of $k(\sqrt{m})$ or not.

§65. The Character Set of an Ideal

Suppose there are t distinct rational prime numbers, $l_1, l_2, \ldots, l_t$ which divide the discriminant of the field $k(\sqrt{m})$. To each rational integer a correspond the completely determined values (= +1 or −1) of the t symbols

$$\left(\frac{a, m}{l_1}\right), \ldots, \left(\frac{a, m}{l_t}\right)$$

as defined in the previous section. These t units ± 1 form the *character set* of the number a in the field $k(\sqrt{m})$. In order to associate a character set also with each ideal $\mathfrak{a}$ of the field $k(\sqrt{m})$ we distinguish the cases where k is an imaginary or a real field. In the first case the norms of the numbers in $k(\sqrt{m})$ are all positive; we set $r = t$, $\bar{n} = +n(\mathfrak{a})$ and say that the r units

$$\left(\frac{\bar{n}, m}{l_1}\right), \ldots, \left(\frac{\bar{n}, m}{l_r}\right) \tag{17.12}$$

form the *character set* of the ideal $\mathfrak{a}$; it is completely and uniquely determined by the ideal $\mathfrak{a}$. In the second case we form first the character set of the number -1,

$$\left(\frac{-1, m}{l_1}\right), \ldots, \left(\frac{-1, m}{l_t}\right). \tag{17.13}$$

If all these units are equal to $+1$ then, as in the first case, we set $\bar{n} = +n(\mathfrak{a})$, $r = t$ and say that the r units (17.12) form the *character set* of the ideal $\mathfrak{a}$. If, on the other hand, the unit -1 occurs among the t characters (17.13), say $\left(\frac{-1, m}{l_t}\right) = -1$, then we set $r = t - 1$ and $\bar{n} = \pm n(\mathfrak{a})$ with the sign so chosen that $\left(\frac{\bar{n}, m}{l_t}\right) = +1$; then the r units (17.12) corresponding to this choice of r and $\bar{n}$ are said to form the *character set* of the ideal $\mathfrak{a}$.

§66. The Character Set of an Ideal Class and the Concept of Genus

Theorem 99. *All the ideals of a single class in the field $k(\sqrt{m})$ have the same character set.*

Proof. If $\mathfrak{a}$ and $\mathfrak{a}'$ are ideals of $k(\sqrt{m})$ belonging to the same class there exists an integer or fraction α in $k(\sqrt{m})$ such that $\mathfrak{a}' = \alpha\mathfrak{a}$. Then we have $n(\mathfrak{a}') = \pm n(\alpha) n(\mathfrak{a})$ where $\pm$ denotes the sign of $n(\alpha)$ and hence

$$\left(\frac{n(\mathfrak{a}'), m}{l}\right) = \left(\frac{\pm n(\mathfrak{a}), m}{l}\right)$$

for $l = l_1, \ldots, l_t$. Referring to the definitions in Sect. 65 we immediately obtain the result of Theorem 99.

In this way a fixed character set is associated with each ideal class. Each collection of ideal classes with the same character set is said to form a *genus*; in particular we define the *principal genus* to be the collection of all ideal classes for which the character set consists entirely of positive units. Since the character set of the principal class clearly has this property it follows that the principal class belongs to the principal genus. From the formula (17.7) on p. 122 we deduce easily that multiplication of the ideal classes from two genera produces the ideal classes of a genus whose character set is obtained by multiplication of the character sets of the two genera. In particular, since the character set of the square of an ideal class chosen from any genus consists entirely of positive units, it follows that the square of every ideal class belongs to the principal genus.

Clearly all the genera contain the same number of classes.

§67. The Fundamental Theorem on the Genera of Quadratic Fields

The question now arises whether an arbitrary set of r units ± 1 can be the character set of a genus of the field $k(\sqrt{m})$. The answer to this question is of fundamental importance for the theory of quadratic fields; it is given in the following theorem, the proof of which will occupy us until Sect. 78.

Theorem 100. *An arbitrary set of r units ± 1 is the character set of a genus of the field $k(\sqrt{m})$ if and only if the product of all r units is $+1$. The number of genera in the field $k(\sqrt{m})$ is thus 2^{r-1} (Gauss (1)).*

§68. A Lemma on Quadratic Fields Whose Discriminants are Divisible by Only One Prime

In order to approach the goal set by Theorem 100 we prove first the following lemma.

Lemma 13. *If the discriminant of a quadratic field $k = k(\sqrt{m})$ has only a single prime factor l then the number of ideal classes in k is odd. The character set for the field k consists of a single character, that associated with the prime l; this character always takes the value $+1$, i.e. there is only one genus in the field k, the principal genus.*

Proof. We denote by s the automorphism of the field k which replaces each number in k by its conjugate. In the case where $m > 0$ let ε be a fundamental unit of k; $-\varepsilon$, $1/\varepsilon$, $-1/\varepsilon$ are also fundamental units. We prove first that under the hypothesis of the lemma we must have $n(\varepsilon) = \varepsilon \cdot s\varepsilon = -1$. Suppose, to the contrary, that we had $n(\varepsilon) = +1$; then, according to Theorem 90, we could find an integer α of the field k such that $\varepsilon = \alpha/s\alpha$. It would follow that $\alpha = \varepsilon \cdot s\alpha$ and so each prime ideal divisor of α would also divide $s\alpha$. Under the hypothesis of the lemma, if $m > 0$ then $\sqrt{m}$ is the unique non-rational prime factor in k coinciding with its conjugate. Thus we must have either $\alpha = \eta a$ or $\alpha = \eta\sqrt{m}a$ where η is a unit and a is a nonzero rational integer; from this it follows that $\varepsilon = \pm\eta^{1-s} = \pm\eta^2$, and this contradicts the hypothesis that ε is a fundamental unit.

Now we proceed to prove the first part of the lemma. If the class number h of the field k were an even number it would follow from Theorem 57 that there would be an ideal $\mathfrak{i}$ of k, not belonging to the principal class, such that $\mathfrak{i}^2 \sim 1$; since $\mathfrak{i} \cdot s\mathfrak{i} \sim 1$ it would follow that $\mathfrak{i} \sim s\mathfrak{i}$. If we set $\mathfrak{i} = \alpha \cdot s\mathfrak{i}$ or $\mathfrak{i}^{1-s} = \alpha$, we see that α is a number in k whose norm $n(\alpha)$ must be ± 1. In the case where $n(\alpha) = +1$ we set $\beta = \alpha$; as we have seen above the possibility that $n(\alpha) = -1$ can occur only where k is a real field and in this case we

set $\beta = \varepsilon\alpha$ where ε, as before, is a fundamental unit of k. In both situations we would have $n(\beta) = +1$ and hence, according to Theorem 90, $1/\beta = \gamma^{1-s}$ where γ is an integer in k. Since $\alpha = \mathfrak{i}^{1-s}$ it would follow that $(\gamma\mathfrak{i})^{1-s} = 1$, i.e. $(\gamma)\mathfrak{i} = s(\gamma\mathfrak{i})$; from this we would deduce in the same way as before that the ideal $(\gamma)\mathfrak{i}$ must be either (a) or $(a)\mathfrak{l}$ where a is a rational integer and $\mathfrak{l}$ the unique non-rational prime factor of k which coincides with its conjugate. Now for $m \neq -1$ this prime factor $\mathfrak{l} = \sqrt{m}$ and for $m = -1$ obviously $\mathfrak{l} = 1 + \sqrt{-1}$; thus we have $\mathfrak{l} \sim 1$. From this it would follow that $\mathfrak{i} \sim 1$, which contradicts the definition of $\mathfrak{i}$.

If k is a real field it follows at once from $n(\varepsilon) = -1$ that

$$\left(\frac{-1, m}{l}\right) = +1$$

and consequently, according to Sect. 65, in each case the character set for an ideal $\mathfrak{i}$ of the field k consists of the single unit $\left(\frac{+n(\mathfrak{i}), m}{l}\right)$. This one character has the value $+1$ for each ideal $\mathfrak{i}$ of k; for, if not, the collection of ideal classes of k would fall into two genera and so the class number h would be even.

Lemma 13 which we have just proved shows that the fundamental Theorem 100 is valid in the simplest case, namely for those quadratic fields whose discriminants have only a single rational prime factor.

§69. The Quadratic Reciprocity Law. A Lemma on the Symbol $\left(\frac{n, m}{w}\right)$

Theorem 101. *Let p and q be distinct positive odd rational prime numbers. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}. \tag{17.14}$$

In addition we have

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \tag{17.15}$$

and

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}. \tag{17.16}$$

(*Gauss* (1)).

d the *quadratic reciprocity law*, (17.15) and (17.16) the two lementary laws.

Proof. If $k(\sqrt{m})$ is a field whose discriminant has only one prime factor l and n is the norm of an ideal of this field k then, according to Lemma 13, we have $\left(\frac{n,m}{l}\right) = +1$. Now, according to Theorem 96 or 97, each positive odd prime not dividing m for which m is a quadratic residue is the norm of an ideal in $k(\sqrt{m})$. Using this fact we obtain the following table in which p and p' are any distinct positive rational prime numbers congruent to 1 modulo 4, q and q' are any distinct positive rational prime numbers congruent to 3 modulo 4, while r is any odd positive rational prime number with no condition imposed on its residue modulo 4.

				If	then
	m	l	n	$\left(\frac{m}{n}\right) = +1$	$\left(\frac{n,m}{l}\right) = +1$
1.	-1	2	r	$\left(\frac{-1}{r}\right) = +1$	$\left(\frac{r,-1}{2}\right) = (-1)^{(r-1)/2} = +1$
2.	2	2	r	$\left(\frac{2}{r}\right) = +1$	$\left(\frac{r,2}{2}\right) = (-1)^{(r^2-1)/8} = +1$
3.	p	p	p'	$\left(\frac{p}{p'}\right) = +1$	$\left(\frac{p',p}{p}\right) = \left(\frac{p'}{p}\right) = +1$
4.	p	p	q	$\left(\frac{p}{q}\right) = +1$	$\left(\frac{q,p}{p}\right) = \left(\frac{q}{p}\right) = +1$
5.	$-q$	q	p	$\left(\frac{-q}{p}\right) = +1$	$\left(\frac{p,-q}{q}\right) = \left(\frac{p}{q}\right) = +1$
6.	$-q$	q	q'	$\left(\frac{-q}{q'}\right) = +1$	$\left(\frac{q',-q}{q}\right) = \left(\frac{q'}{q}\right) = +1$

For a field $k(\sqrt{p})$ it follows from $n(\varepsilon) = -1$ that $\left(\frac{-1}{p}\right) = +1$. Taking this fact together with row 1 of the above table we obtain the general result that $\left(\frac{-1}{r}\right) = (-1)^{(r-1)/2}$. If we apply to the prime 2 the facts quoted at the

start of the proof and bear in mind that the number 2 is the norm of an ideal in $k(\sqrt{p})$ or in $k(\sqrt{-q})$ whenever $(-1)^{(p^2-1)/8} = +1$ or $(-1)^{(q^2-1)/8} = +1$ respectively then, under the latter conditions, it follows that $\left(\frac{2,p}{p}\right) = \left(\frac{2}{p}\right) = +1$ or $\left(\frac{2,-q}{q}\right) = \left(\frac{2}{q}\right) = +1$ respectively; so if $(-1)^{(r^2-1)/8} = +1$ we have $\left(\frac{2}{r}\right) = +1$. Taking this result together with row 2 of the table we see that in general $\left(\frac{2}{r}\right) = (-1)^{(r^2-1)/8}$. From row 3 it follows that $\left(\frac{p}{p'}\right) = \left(\frac{p'}{p}\right)$ and from rows 4 and 5 that $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.

From row 6 we deduce only that if $\left(\frac{-q}{q'}\right) = +1$ then $\left(\frac{q'}{q}\right) = +1$ also. To prove the reciprocity law for two rational primes q and q' both congruent to 3 modulo 4 the easiest approach is to consider the quadratic field $k(\sqrt{qq'})$. Since $\left(\frac{-1,qq'}{q}\right) = -1$ the norm of the fundamental unit ε of this field must be $+1$. So, according to Theorem 90, there is an integer α in $k(\sqrt{qq'})$ such that $\varepsilon = \alpha^{1-s} = \alpha/s\alpha$, where $s\alpha$ is the conjugate of α. From this we conclude easily that the ambig prime ideal $\mathfrak{q}$ dividing q must be a principal ideal. Consequently by suitable choice of the signs we have

$$\left(\frac{\pm q,qq'}{q}\right) = +1 \quad \text{and} \quad \left(\frac{\pm q,qq'}{q'}\right) = +1$$

and hence in each case

$$\left(\frac{q,qq'}{q}\right) = \left(\frac{q,qq'}{q'}\right).$$

This shows, by means of formula (17.5) in Theorem 98 that

$$-\left(\frac{q'}{q}\right) = \left(\frac{q}{q'}\right).$$

Lemma 14. *Let n and m be rational integers, not both negative. Then*

$$\prod_{(w)}\left(\frac{n,m}{w}\right) = +1.$$

where the product on the left hand side is taken over all rational prime numbers w.

Proof. Let p and q be distinct odd rational prime numbers. Then, according to rules (17.2), (17.3) and (17.4) in Sect. 64 and Theorem 101, we have

$$\left(\frac{-1,2}{2}\right) = +1, \quad \left(\frac{-1,p}{2}\right)\left(\frac{-1,p}{p}\right) = +1,$$
$$\left(\frac{2,2}{2}\right) = +1, \quad \left(\frac{2,p}{2}\right)\left(\frac{2,p}{p}\right) = +1,$$
$$\left(\frac{p,p}{2}\right)\left(\frac{p,p}{p}\right) = +1, \quad \left(\frac{p,q}{2}\right)\left(\frac{p,q}{p}\right)\left(\frac{p,q}{q}\right) = +1;$$

using rule (17.1) of Sect. 64 we deduce Lemma 14 for the case where the numbers n, m are ± 1 or contain only one prime factor. According to the formulæ (17.7) and (17.8) of Sect. 64 Lemma 14 follows in general.

It follows also, since $\left(\frac{-1,-1}{2}\right) = -1$, that if n and m are both negative then the corresponding product $\prod_{(w)}$ has the value -1. This assertion and that of Lemma 14 can be given a single formulation if we make use of the new symbol $\left(\frac{n,m}{-1}\right) = \pm 1$, where on the right hand side we take the positive or negative sign according as at least one of the two integers n, m is positive or both are negative.

§70. Proof of the Relation Asserted in Theorem 100 Between All the Characters of a Genus

Lemma 14, which we have just proved in Sect. 69, serves to establish one part of our fundamental Theorem 100. Let A be any ideal class of the field $k(\sqrt{m})$; let $\mathfrak{a}$ be any ideal in A prime to 2 and d; let $\bar{n} = \pm n(\mathfrak{a})$ be the norm of the ideal $\mathfrak{a}$ prefixed by a sign chosen according to Sect. 65. Then the product of all the characters of the class A is given by the expression

$$\left(\frac{\bar{n},m}{l_1}\right)\cdots\left(\frac{\bar{n},m}{l_r}\right).$$

Since $n(\mathfrak{a})$ is the norm of an ideal each rational prime number p occurring to an odd power in $\bar{n}$ must split in $k(\sqrt{m})$; hence, according to Theorem 96, m is a quadratic residue modulo each such prime p. From Lemma 14 and formulæ (17.7), (17.1) and (17.2) of Theorem 98 it follows that

$$\prod_{(w)}\left(\frac{\bar{n},m}{w}\right) = +1,$$

where w runs through all odd prime numbers dividing m and the prime number 2.

If the prime number 2 divides the discriminant of the field $k(\sqrt{m})$ this shows already that for every class in $k(\sqrt{m})$ the product of all characters is $+1$.

If, on the other hand, the prime number 2 does not divide d then, since $m \equiv 1$ modulo 4, we always have $\left(\frac{\bar{n}, m}{2}\right) = +1$ and hence in this case also we have the desired result.

According to the proof we have just given that the product of all the characters is $+1$, we see at once that the number of genera in the quadratic field $k(\sqrt{m})$ is at most half the number of conceivable character sets, i.e. can be at most 2^{r-1}.

18. Existence of Genera in Quadratic Fields

§71. Theorem on the Norms of Numbers in a Quadratic Field

It still remains for us to establish the second part of the fundamental Theorem 100, i.e. to prove that the condition we have just proved necessary for a set of r units ± 1 to be the character set of a genus in $k(\sqrt{m})$ is also sufficient. This proof can be carried out in two completely different ways: the first is purely arithmetic in nature, the second makes essential use of transcendental methods. The first proof is achieved through the following considerations.

Theorem 102.[1] *If n and m are rational integers such that m is not a square and such that*

$$\left(\frac{n,m}{w}\right) = +1$$

for every prime number w, then n is the norm of an integer or fraction in the field $k(\sqrt{m})$.

Proof. Since $\prod_{(w)} \left(\frac{n,m}{w}\right) = +1$ it follows from the remark on page 131 that at least one of the integers n, m is positive. We may suppose that n and m have no rational square factors. If p is a prime number dividing n which also divides the discriminant d of the field $k(\sqrt{m})$, then p is the norm of an ideal in $k(\sqrt{m})$. Further, if p is an odd prime number which divides n but not m then, since

$$\left(\frac{n,m}{p}\right) = \left(\frac{m}{p}\right) = +1,$$

the prime number p is again the norm of an ideal in $k(\sqrt{m})$. Finally, if the prime number 2 divides n but not the discriminant of $k(\sqrt{m})$ then, since

$$\left(\frac{n,m}{2}\right) = \left(\frac{2,m}{2}\right) = (-1)^{(m^2-1)/8} = +1,$$

[1] The criteria for the solvability of ternary quadratic diophantine equations were first discovered by Lagrange (*Lagrange* (1)).

we have again that 2 is the norm of an ideal in $k(\sqrt{m})$ and hence it follows that there is an ideal $\mathfrak{i}$ of $k(\sqrt{m})$ such that $|n| = n(\mathfrak{i})$. Now we choose an ideal $\mathfrak{i}'$ in the ideal class determined by $\mathfrak{i}$ whose norm $n(\mathfrak{i}') \leq |\sqrt{d}\,|$, where d is the discriminant of the field $k(\sqrt{m})$. (According to Theorem 50 this is always possible.) We set $\mathfrak{i}' = \kappa\mathfrak{i}$ and $n' = n \cdot n(\kappa)$ where κ is an integer or fraction in $k(\sqrt{m})$ and $n' = \pm n(\mathfrak{i}')$ where we take the positive or negative sign according as $n \cdot n(\kappa)$ is positive or negative. In particular the rational integer n' is certainly positive if m is negative. Since d is either m or $4m$ we certainly have $|n'| < 2|\sqrt{m}|$ and hence $|n'| \leq |m|$ as soon as $2|\sqrt{m}| < |m|$, i.e. $|m| > 4$. On the other hand, since $n' = n \cdot n(\kappa)$ we have $\left(\frac{n, m}{w}\right) = \left(\frac{n', m}{w}\right) = +1$ and hence, by formula (17.6) in Theorem 98, we have $\left(\frac{m, n'}{w}\right) = +1$ for all prime numbers w.

We now make the hypothesis that the conclusion of Theorem 102 holds for each field $k(\sqrt{m'})$ such that m' (whether positive or negative) satisfies the inequality $|m'| < |m|$. As soon as the number n' introduced above satisfies the inequality $|n'| < |m|$ and is not a square then, since the condition $\left(\frac{m, n'}{w}\right) = +1$ holds for every prime number w, it follows from our hypothesis that m is the norm of a number α' in the field $k(\sqrt{n'})$. Thus there are two rational numbers a and b such that $m = a^2 - n'b^2$; of course if n' is a square the solvability of this equation is immediately clear. Since b must be nonzero it follows that $n' = (a/b)^2 - m(1/b)^2 = n(\lambda)$, i.e. n' is the norm of a number λ in the field $k(\sqrt{m})$. Combining this fact with the equation $n' = n \cdot n(\kappa)$ we see that $n = n(\alpha)$ where $\alpha = \lambda/\kappa$ is again a number in $k(\sqrt{m})$.

The proof of Theorem 102 will accordingly be completed as soon as we can show that it holds for all cases in which $|m| \leq 4$ and $|n| \leq |\sqrt{d}\,|$. There are only 8 cases satisfying these conditions and the equations

$$\begin{aligned} 1 &= n(\sqrt{-1}), & -2 &= n(\sqrt{2}), \\ 2 &= n(1+\sqrt{-1}), & 2 &= n(\sqrt{-2}), \\ 2 &= n(2+\sqrt{2}), & -2 &= n(1+\sqrt{3}), \\ -1 &= n(1+\sqrt{2}), & -3 &= n(\sqrt{3}) \end{aligned}$$

show that in these 8 cases Theorem 102 is valid.

We see easily that Theorem 102 is also valid if we require that the condition $\left(\frac{n, m}{w}\right) = +1$ hold only for all odd primes w, provided we impose the additional condition that at least one of the numbers n, m is positive. (*Lagrange* (1), *Legendre* (1), *Gauss* (1)); in fact, according to Lemma 14, the remaining condition $\left(\frac{n, m}{2}\right) = +1$ is automatically fulfilled in this case.

§72. The Classes of the Principal Genus

At the end of Sect. 66 we showed that the square of each ideal class belongs to the principal genus. Theorem 102 of Sect. 72 gives us the means of proving the converse result.

Theorem 103. *Every ideal class in the principal genus of a quadratic field is the square of a class* (*Gauss* (1)).

Proof. Let H be a class in the principal genus of the field $k(\sqrt{m})$, $\mathfrak{h}$ an ideal in the class H which is prime to the discriminant d of $k(\sqrt{m})$ and $\bar{n}$ the norm of the ideal $\mathfrak{h}$ with the appropriate sign attached according to Sect. 65. Then this number $\bar{n}$ satisfies the condition $\left(\frac{\bar{n}, m}{w}\right) = +1$ for each prime number w and hence, by Theorem 102, $\bar{n} = n(\alpha)$, where α is an integer or fraction in the field $k(\sqrt{m})$. If we set $\mathfrak{h}/\alpha = \mathfrak{k}/\mathfrak{k}'$, where $\mathfrak{k}$ and $\mathfrak{k}'$ are ideals prime to one another it follows that $\frac{\mathfrak{k} \cdot s\mathfrak{k}}{\mathfrak{k}' \cdot s\mathfrak{k}'} = 1$ and hence we must have $\mathfrak{k}' = s\mathfrak{k}$. Since $\mathfrak{k} \cdot s\mathfrak{k} \sim 1$ it follows that $\mathfrak{h} \sim \mathfrak{k}^2$.

The characteristic property of the ideals in the principal genus which we have just established is closely associated with another property, also characteristic, which we state in the following theorem.

Theorem 104. *Let ω_1 and ω_2 form a basis for the quadratic field k and let η_1 and η_2 form a basis for an ideal $\mathfrak{h}$ in the principal genus of k. If N is any rational integer we can always find four rational numbers r_{11}, r_{12}, r_{21}, r_{22} whose denominators are prime to N and with determinant $r_{11}r_{22} - r_{12}r_{21} = \pm 1$ such that*

$$\frac{\eta_1}{\eta_2} = \frac{r_{11}\omega_1 + r_{12}\omega_2}{r_{21}\omega_1 + r_{22}\omega_2}.$$

Proof. Let $\mathfrak{h}' = \beta\mathfrak{h}$ be an ideal equivalent to $\mathfrak{h}$ which is prime to Nd. As in the proof of Theorem 103 $\bar{n} = \pm n(\mathfrak{h}')$, with the sign chosen as in Sect. 65, is equal to the norm of a number α in the field k. Here α may be so chosen that there is a rational integer r prime to Nd such that $r\alpha$ is an integer of k. The ideal $r\alpha\mathfrak{h}' = r\alpha\beta\mathfrak{h}$ has as basis

$$r\alpha\beta\eta_1 = a_{11}\omega_1 + a_{12}\omega_2,$$
$$r\alpha\beta\eta_2 = a_{21}\omega_1 + a_{22}\omega_2,$$

where a_{11}, a_{12}, a_{21}, a_{22} are rational integers. Since $n(\alpha\mathfrak{h}') = \bar{n}^2$ the determinant $a_{11}a_{22} - a_{12}a_{21} = \pm r^2\bar{n}^2$ and hence the four numbers $r_{11} = a_{11}/r\bar{n}$, $r_{12} = a_{12}/r\bar{n}$, $r_{21} = a_{21}/r\bar{n}$, $r_{22} = a_{22}/r\bar{n}$ have the property required in the theorem.

§73. Ambig Ideals

An ideal $\mathfrak{a}$ of a quadratic field k is called an *ambig ideal* if it is invariant under the substitution $s = (\sqrt{m} : -\sqrt{m})$ and has no rational integer factor other than ± 1 (cf. Sect. 57). We have the following result.

Theorem 105. *The t distinct prime ideals $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$ which divide the discriminant d of the field k, and only these, are ambig prime ideals of k. The 2^t ideals $1, \mathfrak{l}_1, \mathfrak{l}_2, \ldots, \mathfrak{l}_1\mathfrak{l}_2, \ldots, \mathfrak{l}_1\mathfrak{l}_2\ldots\mathfrak{l}_t$ form the totality of all ambig ideals of the field k.*

Proof. It follows from Theorem 96 that $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$, and only these, are ambig prime ideals. Now let $\mathfrak{a} = \mathfrak{p}\mathfrak{q}\ldots\mathfrak{r}$ be an ambig ideal, expressed as a product of prime ideals. Since $s\mathfrak{a} = \mathfrak{a}$ it follows that the prime ideals $s\mathfrak{p}$, $s\mathfrak{q}$, $\ldots$, $s\mathfrak{r}$ conjugate to $\mathfrak{p}, \mathfrak{q}, \ldots, \mathfrak{r}$ must coincide up to order with $\mathfrak{p}, \mathfrak{q}, \ldots, \mathfrak{r}$. Suppose it turns out that $s\mathfrak{p} = \mathfrak{q}$ where $\mathfrak{q} \neq \mathfrak{p}$; then $\mathfrak{a}$ would have the factor $\mathfrak{p}\cdot s\mathfrak{p}$, which is a rational integer. Since this contradicts the definition of ambig ideals it follows that we must have $s\mathfrak{p} = \mathfrak{p}$ and similarly $s\mathfrak{q} = \mathfrak{q}, \ldots, s\mathfrak{r} = \mathfrak{r}$, i.e. the prime ideals $\mathfrak{p}, \mathfrak{q}, \ldots, \mathfrak{r}$ are all ambig. Since the squares of the ideals $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$ are all rational integers we conclude that the ideals $\mathfrak{p}, \mathfrak{q}, \ldots, \mathfrak{r}$ must all be distinct. Hence we have the latter part of Theorem 105.

§74. Ambig Ideal Classes

If $\mathfrak{a}$ is an ideal in the ideal class A then the class to which the ideal $s\mathfrak{a}$ belongs is denoted by sA. If it happens that $sA = A$ we say that A is an *ambig ideal class*. Since the product $\mathfrak{a} \cdot s\mathfrak{a} \sim 1$ it follows that $A \cdot sA = 1$; consequently the square of each ambig ideal class is the principal class 1. Conversely, if the square of a class A is equal to 1 then $A = 1/A = sA$ and hence A is an ambig class.

§75. Ambig Classes Determined by Ambig Ideals

There now arises the problem of determining all the ambig classes of k. It is clear that each ambig ideal $\mathfrak{a}$, in virtue of the property that $s\mathfrak{a} = \mathfrak{a}$, determines an ambig class; so we have first to investigate how many distinct ambig classes arise from the 2^t ambig ideals. We call a set of ideal classes *independent* if it does not contain the principal class 1 and if none of the classes in the set can be expressed as a product of powers of the others. Then we can state the following result.

Theorem 106. *In the case of an imaginary quadratic field the t ambig prime ideals determine $t-1$ independent ambig classes. In the case of a real*

quadratic field they determine either $t-2$ or $t-1$ independent ambig classes according as the norm of the fundamental unit ε is $+1$ or -1. The 2^t ambig ideals determine in the imaginary case 2^{t-1} distinct ambig classes and in the real case either 2^{t-2} or 2^{t-1} distinct ambig classes according as $n(\varepsilon) = +1$ or -1.

Proof. The product of all the prime ideals dividing m is equal to $\sqrt{m}$ and hence is a principal ideal of k.

First suppose that m is negative but distinct from -1 and -3. Let (α) be an ambig principal ideal in k. Then α^{1-s}, being a unit, must be $(-1)^e$ where e is either 0 or 1; from this it follows that

$$\{\alpha(\sqrt{m})^e\}^{1-s} = 1 \qquad \text{or} \qquad \alpha(\sqrt{m})^e = s(\alpha(\sqrt{m})^e),$$

and so $\alpha(\sqrt{m})^e$ is a rational integer. This shows that in an imaginary field $k(\sqrt{m})$ – other than $k(\sqrt{-1})$ or $k(\sqrt{-3})$ – there are no ambig principal ideals apart from 1 and $\sqrt{m}$. The two excluded cases are immediately dealt with.

In establishing the result in question for a real field k the important thing is whether the norm of the fundamental unit ε is $+1$ or -1.

If $n(\varepsilon) = +1$ then, according to Theorem 90, the equation $\varepsilon = \alpha^{1-s}$ is satisfied by an integer α in k, and we may suppose further that α has no rational factor other than ± 1. Since $\alpha = \varepsilon \cdot s\alpha$ it follows that (α) is an ambig principal ideal. This principal ideal is distinct from 1 and $\sqrt{m}$; for if α were $\pm\varepsilon^f$ or $\pm\varepsilon^f\sqrt{m}$, where the exponent f is a rational integer, we would have

$$\alpha^{1-s} = (-1)^e \varepsilon^{(1-s)f} = (-1)^e \varepsilon^{2f}$$

where $e = 0$ or 1 respectively; this unit is, however, always distinct from ε. If α' is an arbitrary ambig principal ideal of the field k we must have $(\alpha')^{1-s} = (-1)^e\varepsilon^f$, where e and f are rational integers. If we set $\alpha'' = \alpha'/(\sqrt{m})^e\alpha^f$ we have $(\alpha'')^{1-s} = 1$ and hence α'' is a rational number. Thus apart from 1, $\sqrt{m}$ and α there is only one ambig principal ideal which is obtained by removing any rational integer factors other than ± 1 from the product $\sqrt{m}\alpha$.

On the other hand, if $n(\varepsilon) = -1$, there is no ambig principal ideal in k distinct from 1 and $\sqrt{m}$; for if (α) is an ambig principal ideal we necessarily have an equation of the form $(\alpha)^{1-s} = (-1)^e\varepsilon^f$ where e and f are rational integers. Since $n(\alpha^{1-s}) = +1$ it follows that $(n(\varepsilon))^f = +1$ and so f is an even number. If we set

$$\alpha' = \frac{\alpha}{\varepsilon^{f/2}(\sqrt{m})^{e+f/2}}$$

it follows that $(\alpha')^{1-s} = +1$ and so α' is a rational number.

We now express a suitably chosen one of the t ambig prime ideals by means of $\sqrt{m}$ and the remaining $t-1$ ambig prime ideals; and, if k is real and $n(\varepsilon) = +1$ a suitable one of these $t-1$ ambig prime ideals by means of α and the remaining $t-2$ ambig prime ideals. Thus we have established the second part of Theorem 106.

§76. Ambig Ideal Classes Containing no Ambig Ideals

We have the following result.

Theorem 107. *A quadratic field k has an ambig ideal class containing no ambig ideal if and only if k is real, the character set of -1 in k consists entirely of positive units and further the norm of the fundamental unit is $+1$. If these conditions are satisfied then all ideal classes of this type are obtained by multiplying any chosen one of them by all the ideal classes arising from ambig ideals.*

Proof. If the field k is real and the character set of -1 in k consists entirely of positive units then, according to Theorem 102, there exists an integer or fraction α in k with norm -1. If in addition we have $n(\varepsilon) = +1$ then this number α must be a fraction. Set $\alpha = \mathfrak{i}/\mathfrak{i}'$ where $\mathfrak{i}$ and $\mathfrak{i}'$ are relatively prime ideals. Then $\frac{\mathfrak{i} \cdot s\mathfrak{i}}{\mathfrak{i}' \cdot s\mathfrak{i}'} = 1$ from which we deduce that $\mathfrak{i}' = s\mathfrak{i}$ and hence $\mathfrak{i} \sim s\mathfrak{i}$, so that $\mathfrak{i}$ determines an ambig class. We claim that this ambig class contains no ambig ideal. For if there were an ambig ideal $\mathfrak{a} = \mathfrak{i}\beta$, where β is an integer or fraction in k, we would have $\mathfrak{a}^{1-s} = \alpha\beta^{1-s}$ and hence $\alpha\beta^{1-s}$ would be a unit, say $\alpha\beta^{1-s} = (-1)^e\varepsilon^f$, and consequently $n(\alpha) = 1$, which contradicts the defining property of the number α. Thus we have proved that the ideal class determined by $\mathfrak{i}$ contains no ambig ideal.

Now let A be any ambig ideal class and $\mathfrak{i}$ an ideal in A, so that $\mathfrak{i}^{1-s}$ is equal to an integer or fraction α of the field k and the norm of α is either $+1$ or -1. The first case is the only one possible if the field k is imaginary or if k is real and at least one of the characters $\left(\frac{-1, m}{w}\right)$ has the value -1. If $n(\alpha) = +1$ it follows that $1/\alpha = \beta^{1-s}$ where β is an integer in k; then we have $(\mathfrak{i}\beta)^{1-s} = 1$, i.e. $\mathfrak{i}\beta$ is equal to the product of an ambig ideal with a rational number and so the class A contains an ambig ideal. On the other hand if $n(\alpha) = -1$ and $n(\varepsilon) = -1$ then $n(\varepsilon\alpha) = +1$ and we prove as before that the class A contains an ambig ideal. Thus we see that in the cases (1) where k is imaginary and (2) where k is real and either one of the characters of -1 has the value -1 or else $n(\varepsilon) = -1$, each ambig ideal class contains an ambig ideal.

Finally suppose in the case where none of these conditions holds that there are several ambig ideal classes in k containing no ambig ideals. Choose ideals $\mathfrak{i}$ and $\mathfrak{i}'$ from two such classes; then our earlier discussion shows that the norms of the numbers $\alpha = \mathfrak{i}^{1-s}$ and $\alpha' = \mathfrak{i}'^{1-s}$ must have the value -1 and so $n(\alpha'/\alpha) = +1$. By Theorem 90 we can write $\alpha'/\alpha = \beta^{1-s}$ where β is a suitable integer in k. If we set $\frac{\mathfrak{i}'\beta}{\mathfrak{i}} = b\mathfrak{a}$, where b is a rational number and $\mathfrak{a}$ is an ideal with no rational integer factor other than ± 1, it follows from

the equation $\left(\frac{\mathfrak{i}'\beta}{\mathfrak{i}}\right)^{1-s} = 1$ that $\mathfrak{a} = s\mathfrak{a}$, i.e. that $\mathfrak{a}$ is an ambig ideal. Then $\mathfrak{i}' \sim \mathfrak{i}\mathfrak{a}$ and so we have proved the last part of Theorem 107.

§77. The Number of All Ambig Ideal Classes

Theorems 106 and 107 make possible the calculation of the number of all ambig ideal classes.

Theorem 108. *In every case there exist $r-1$ independent ambig ideal classes, where r is the number of individual characters which determine the genus of a class. The total number of distinct ambig ideal classes is thus 2^{r-1}.*

Proof. As before, let t be the number of distinct rational prime numbers dividing the discriminant d of the field k. We consider first the case where k is an imaginary field; here it follows from Theorems 106 and 107 that there are precisely 2^{t-1} ambig classes in k, which all arise from ambig ideals. Next suppose that k is a real field. If the character set of -1 in k consists entirely of positive units it follows again from Theorems 106 and 107 that there are precisely 2^{t-1} ambig classes in k; of these 2^{t-1} classes either all or only half arise from ambig ideals, according as $n(\varepsilon) = -1$ or $+1$. If, on the other hand, the character set of -1 in k contains at least one negative character then $n(\varepsilon) = +1$ and according to Theorems 106 and 107 there are only 2^{t-2} ambig classes in k, all of which arise from ambig ideals. Now when k is real and the number -1 has at least one negative character in k the number r of individual characters is $t-1$; in all other cases we have $r = t$. Thus the proof of Theorem 108 is completed.

§78. Arithmetic Proof of the Existence of Genera

The results we have proved put us in a position to obtain the answer to the question about the number of genera which was raised by the fundamental Theorem 100. Namely we can prove that this number is always 2^{r-1} and that in consequence all those character sets which satisfy the condition of Theorem 100 actually correspond to genera. We denote the number of distinct genera by g and the number of classes in the principal genus by f. Since, according to Sect. 66, all genera contain the same number of classes we see that the total number of ideal classes in the field is $h = gf$. If we denote the f classes in the principal genus by $H_1, \ldots, H_f$ then, according to Theorem 103, we can set $H_1 = K_1^2, \ldots, H_f = K_f^2$, where $K_1, \ldots, K_g$ are certain classes of the field.

Now let C be any ideal class of the field; since C^2 belongs to the principal genus we must have $C^2 = K_a^2$ where K_a is uniquely determined among the classes $K_1, \ldots, K_f$ introduced above. Then C/K_a, i.e. the uniquely determined class A such that $C = AK_a$, is an ambig class. Thus the expression AK where A runs through all the ambig classes and K through the classes $K_1, \ldots, K_f$ represents each ideal class once and once only. According to Theorem 108 the number of ambig ideal classes is 2^{r-1}; hence $h = 2^{r-1}f$ and so, combining this equation with the relation $h = gf$ derived above, we deduce the result that $g = 2^{r-1}$. This completes the proof of the fundamental Theorem 100 (*Gauss* (1)).

§79. Transcendental Representation of the Class Number and an Application that the Limit of a Certain Infinite Product is Positive

The second proof of the existence of 2^{r-1} genera rests on transcendental foundations; we develop the following sequence of theorems.

Theorem 109. *The number h of ideal classes of a quadratic field k with discriminant d is given by the formula*

$$\kappa h = \lim_{s=1} \prod_{(p)} \frac{1}{1 - \left(\frac{d}{p}\right)p^{-s}}.$$

Here the product on the right hand side is taken over all rational prime numbers p and the symbol $\left(\frac{d}{p}\right)$ has the meaning described in Sect. 61. *The factor κ is given by*

$$\kappa = \frac{2\pi}{w|\sqrt{d}\,|} \qquad \text{or} \qquad \kappa = \frac{2\log\varepsilon}{|\sqrt{d}\,|}$$

according as k is imaginary or real, i.e. according as d is negative or positive. For $d = -3$ we take $w = 6$; for $d = -4$ we take $w = 4$; for all other negative discriminants d we take $w = 2$. For a real field we take ε to be that one of its four fundamental units which is > 1; and by $\log\varepsilon$ we mean the real value of the logarithm of this fundamental unit ε (Dirichlet (8, 9)).

Proof. According to Sect. 27 we have, for all real numbers $s > 1$,

$$\zeta(s) = \sum_{(\mathfrak{i})} \frac{1}{n(\mathfrak{i})^s} = \prod_{(\mathfrak{p})} \frac{1}{1 - (n(\mathfrak{p}))^{-s}},$$

where the product is taken over all prime ideals $\mathfrak{p}$ of k. Let us arrange the factors of this product according to the rational prime numbers p from which the prime ideals $\mathfrak{p}$ are derived; then, as we deduce from Theorem 97, to each rational prime number p corresponds the factor

$$\frac{1}{(1-p^{-s})^2} \quad \text{or} \quad \frac{1}{(1-p^{-2s})} \quad \text{or} \quad \frac{1}{1-p^{-s}}$$

according as $\left(\dfrac{d}{p}\right) = +1$ or -1 or 0. We can write these three expressions in a common form

$$\frac{1}{1-p^{-s}} \cdot \frac{1}{1 - \left(\dfrac{d}{p}\right)p^{-s}}$$

and so obtain

$$\zeta(s) = \prod_{(p)} \frac{1}{1-p^{-s}} \cdot \prod_{(p)} \frac{1}{1 - \left(\dfrac{d}{p}\right)p^{-s}}$$

where the products on the right hand side are taken over all rational prime numbers p. Since

$$\lim_{s=1} \left\{ (s-1) \prod_{(p)} \frac{1}{1-p^{-s}} \right\} = \lim_{s=1} \left\{ (s-1) \sum_{(n)} \frac{1}{n^s} \right\} = 1,$$

where n runs through all positive rational integers, we have

$$\lim_{s=1} \{(s-1)\zeta(s)\} = \lim_{s=1} \prod_{(p)} \frac{1}{1 - \left(\dfrac{d}{p}\right)p^{-s}}.$$

Theorem 109 now follows from Theorem 56 when we introduce the value of κ given in Sect. 25. To determine w we note that the field $k(\sqrt{-3})$ contains the 6 roots of unity ± 1, $\pm\dfrac{1 \pm \sqrt{-3}}{2}$, the field $k(\sqrt{-1})$ the 4 roots of unity ± 1, $\pm i$, while all remaining imaginary quadratic fields contain only the 2 roots of unity ± 1 (cf. Sect. 62).

The most important consequence of the fact we have just proved is the following theorem.

Theorem 110. *Let a be any positive or negative rational integer, not a square. Then the limit*

$$\lim_{s=1} \prod_{(p)} \frac{1}{1-\left(\frac{a}{p}\right)p^{-s}}$$

is always finite and nonzero (*Dirichlet* (8, 9)).

Proof. Let $a = b^2 m$ where b^2 is the largest square number dividing a; let d be the discriminant of the quadratic field determined by $\sqrt{a}$. Then for each odd rational prime p not dividing b we have $\left(\frac{a}{p}\right) = \left(\frac{d}{p}\right)$. The two infinite products

$$\prod_{(p)} \frac{1}{1-\left(\frac{d}{p}\right)p^{-s}} \quad \text{and} \quad \prod_{(p)} \frac{1}{1-\left(\frac{a}{p}\right)p^{-s}}$$

can thus differ from one another in only finitely many factors. Since, according to Theorem 109, the first product has a finite nonzero limit for $s = 1$ the same holds also for the second product.

§80. Existence of Infinitely Many Rational Prime Numbers Modulo Which Given Numbers Have Prescribed Quadratic Residue Characters

Using Theorem 110 we prove in succession the following results (*Dirichlet* (9), *Kronecker* (10)).

Theorem 111. *Let $a_1, a_2, \ldots, a_t$ be any positive or negative rational integers such that none of the $2^t - 1$ integers $a_1, a_2, \ldots, a_t, a_1a_2, \ldots, a_{t-1}a_t, \ldots, a_1a_2 \ldots a_t$ is a square; let $c_1, c_2, \ldots, c_t$ be any units ± 1 . Then there are infinitely many rational prime numbers p such that*

$$\left(\frac{a_1}{p}\right) = c_1, \left(\frac{a_2}{p}\right) = c_2, \ldots, \left(\frac{a_t}{p}\right) = c_t.$$

Proof. If $s > 1$ we have

$$\log \sum_{(n)} \frac{1}{n^s} = \sum_{(p)} \log \frac{1}{1-p^{-s}} = \sum_{(p)} \frac{1}{p^s} + S$$

where

$$S = \frac{1}{2}\sum_{(p)} \frac{1}{p^{2s}} + \frac{1}{3}\sum_{(p)} \frac{1}{p^{3s}} + \cdots.$$

Since, as we showed in Sect. 50, the expression S remains finite for $s = 1$ it follows that as s approaches 1 the sum

$$\sum_{(p)} \frac{1}{p^s} \tag{18.1}$$

taken over all rational primes p must increase beyond limit. If a is any rational integer then for $s > 1$ we have similarly

$$\log \prod_{(p)} \frac{1}{1 - \left(\frac{a}{p}\right) p^{-s}} = \sum_{(p)} \left(\frac{a}{p}\right) \cdot \frac{1}{p^s} + S_a,$$

where

$$S_a = \frac{1}{2} \sum_{(p)} \left(\frac{a}{p}\right)^2 \cdot \frac{1}{p^{2s}} + \frac{1}{3} \sum_{(p)} \left(\frac{a}{p}\right)^3 \cdot \frac{1}{p^{3s}} + \cdots.$$

If a is not a square then, according to Theorem 110,

$$\log \prod_{(p)} \frac{1}{1 - \left(\frac{a}{p}\right) p^{-s}}$$

has a finite limit at $s = 1$, and since the same holds for the expression S_a it follows also that the sum

$$\sum_{(p)} \left(\frac{a}{p}\right) \cdot \frac{1}{p^s} \tag{18.2}$$

also has a finite limit at $s = 1$. Now in (18.2) we set

$$a = a_1^{u_1} a_2^{u_2} \dots a_t^{u_t}$$

and give each of the t exponents $u_1, u_2, \dots, u_t$ the value 0 or 1, excluding the possibility that $u_1 = u_2 = \dots = u_t = 0$. Suppose that the sum (18.2) for each choice of $u_1, u_2, \dots, u_t$ is multiplied by the corresponding $c_1^{u_1} c_2^{u_2} \dots c_t^{u_t}$ and all the $2^t - 1$ sums so formed are added to (18.1). Then we obtain

$$\sum_{(p)} \left(1 + c_1\left(\frac{a_1}{p}\right)\right)\left(1 + c_2\left(\frac{a_2}{p}\right)\right) \cdots \left(1 + c_t\left(\frac{a_t}{p}\right)\right) \cdot \frac{1}{p^s}. \tag{18.3}$$

This sum, just like (18.1), exceeds all bounds as s approaches 1. If we disregard the terms which correspond to the primes p which divide $a_1 a_2 \dots a_t$ (of which there are only finitely many) the remainder of the sum (18.3) is

$$2^t \sum_{(p')} \frac{1}{(p')^s}$$

where p' runs through all and only the prime numbers p for which the conditions described in Theorem 111 are all satisfied. Since, however, the latter sum also increases beyond all bounds as s approaches 1 it follows that the number of such primes p' must be infinite. This completes the proof of Theorem 111.

§81. Existence of Infinitely Many Prime Ideals with Prescribed Characters in a Quadratic Field

Theorem 112. *Let*

$$\chi_1(\mathfrak{i}) = \left(\frac{\pm n(\mathfrak{i}), m}{l_1}\right), \ldots, \chi_r(\mathfrak{i}) = \left(\frac{\pm n(\mathfrak{i}), m}{l_r}\right)$$

be the r characters which determine the genus of an ideal $\mathfrak{i}$ in k and let $c_1, \ldots, c_r$ be any r units ± 1 such that $c_1 \ldots c_r = +1$. Then there are infinitely many prime ideals $\mathfrak{p}$ in the field k such that

$$\chi_1(\mathfrak{p}) = c_1, \ldots, \chi_r(\mathfrak{p}) = c_r.$$

Proof. Suppose the discriminant d of the field has the t prime factors $l_1, \ldots, l_t$. Here $t = r$ or $t = r + 1$. In the latter case let $\left(\frac{-1, m}{l_t}\right) = -1$ and use the condition $\left(\frac{\pm n(\mathfrak{i}), m}{l_t}\right) = +1$ to determine the sign in $\pm n(\mathfrak{i})$; at the same time we write in this case $c_t = c_{r+1} = +1$.

We prove first that there are infinitely many rational prime numbers p for which

$$\left(\frac{p, m}{l_1}\right) = c_1, \ldots, \left(\frac{p, m}{l_t}\right) = c_t;$$

to do this we distinguish three cases according as m is congruent to 1, 3 or 2 modulo 4.

In the first case ($m \equiv 1 \pmod 4$) we proceed from the requirement that

$$\left(\frac{-1}{p}\right) = +1, \left(\frac{l_1}{p}\right) = c_1, \ldots, \left(\frac{l_t}{p}\right) = c_t.$$

According to Theorem 111 there are infinitely many primes p which satisfy these equations. Since the first equation implies that $p \equiv 1 \pmod 4$, we shall have for these prime numbers p

$$\left(\frac{p, m}{l_i}\right) = \left(\frac{p}{l_i}\right) = \left(\frac{l_i}{p}\right) = c_i$$

for $i = 1, \ldots, t$.

In the second case ($m \equiv 3 \pmod 4$) one of the prime numbers $l_1, \ldots, l_t$, say l_z, is the prime number 2. If $c_z = +1$ we start with the requirements

$$\left(\frac{-1}{p}\right) = +1, \left(\frac{l_i}{p}\right) = c_i \quad (i = 1, \ldots, z-1, z+1, \ldots, t).$$

It follows from Theorem 111 that there are infinitely many prime numbers satisfying these conditions. According to the first condition we have for each

of these prime numbers p that $\left(\frac{p,m}{2}\right) = +1 = c_z$ and further that $\left(\frac{p,m}{l_i}\right) = \left(\frac{p}{l_i}\right) = \left(\frac{l_i}{p}\right) = c_i$ for $i = 1,\dots,z-1,z+1,\dots,t$. If on the other hand we have $c_z = -1$ we consider the conditions

$$\left(\frac{-1}{p}\right) = -1, \left(\frac{l_i}{p}\right) = (-1)^{(l_i-1)/2}c_i \quad (i = 1,\dots,z-1,z+1,\dots,t).$$

Then the infinitely many prime numbers p satisfying these equations also fulfil the conditions

$$\left(\frac{p,m}{2}\right) = -1 = c_z \quad\text{and}\quad \left(\frac{p,m}{l_i}\right) = \left(\frac{p}{l_i}\right) = (-1)^{(l_i-1)/2}\left(\frac{l_i}{p}\right) = c_i$$

for $i = 1,\dots,z-1,z+1,\dots,t$.

In the third case ($m \equiv 2 \pmod 4$) we again set $l_z = 2$. We consider the conditions

$$\left(\frac{-1}{p}\right) = +1, \left(\frac{2}{p}\right) = c_z, \left(\frac{l_i}{p}\right) = c_i \quad (i = 1,\dots,z-1,z+1,\dots,t).$$

Again according to Theorem 111 there are infinitely many prime numbers p which satisfy these conditions and for which it follows that

$$\left(\frac{p,m}{2}\right) = (-1)^{((p^2-1)/8+(p-1)(m/2-1)/4} = (-1)^{(p^2-1)/8)} = \left(\frac{2}{p}\right) = c_z$$

and further $\left(\frac{p,m}{l_i}\right) = \left(\frac{p}{l_i}\right) = \left(\frac{l_i}{p}\right) = c_i$ for $i = 1,\dots,z-1,z+1,\dots,t$.

Now let p be any rational prime number such that

$$\left(\frac{p,m}{l_1}\right) = c_1,\dots,\left(\frac{p,m}{l_t}\right) = c_t.$$

According to Lemma 14 we have

$$\prod_{(w)}\left(\frac{p,m}{w}\right) = \left(\frac{p,m}{p}\right)\left(\frac{p,m}{l_1}\right)\dots\left(\frac{p,m}{l_t}\right) = +1$$

and hence

$$\left(\frac{m}{p}\right)c_1\dots c_t = \left(\frac{m}{p}\right) = +1.$$

Thus p splits in the field k as a product of two prime ideals $\mathfrak{p}$ and $\mathfrak{p}'$. Each of these prime ideals satisfies the conditions of Theorem 112.

§82. Transcendental Proof of the Existence of Genera and the Other Results Obtained in Sections 71 to 77

Theorem 112 not only shows anew the existence of 2^{r-1} genera but also reveals another, deeper, result.

Theorem 113. *Each genus in a quadratic field contains infinitely many prime ideals.*

If we establish the theorem on the existence of 2^{r-1} genera by the second (transcendental) method independently of Theorems 102, 103 and 108, it is easy to deduce these theorems as corollaries. To this end we need only the fact that the number a of ambig classes in k does not exceed 2^{r-1}. This follows from Theorem 106 about the number of ambig classes which derive from ambig ideals together with the results of the second and third paragraphs of the proof of Theorem 107; this line of argument is completely independent of Theorem 102.

As above, let f be the number of classes in the principal genus, g the number of genera and f' the number of classes in the principal genus which are squares of classes. As in Sect. 78 it follows that $gf = af'$ and since it is already established that $g = 2^{r-1}$ we must have $a \leq 2^{r-1}$; clearly $f' \leq f$; so it follows that $f' = f$ and $a = 2^{r-1}$. The first equation proves Theorem 103, the second Theorem 108 and then Theorem 102 for the case where $n = -1$. From this last result and Theorem 103 we deduce Theorem 102 for all n as follows. According to the condition imposed on n in Theorem 102, n is the norm of an ideal $\mathfrak{h}$ of the principal genus equipped with a sign as described in Sect. 65. Let $\mathfrak{k}$ be an ideal such that $\mathfrak{h} \sim \mathfrak{k}^2$. Then $\alpha = \dfrac{\mathfrak{h} \cdot n(\mathfrak{k})}{\mathfrak{k}^2}$ must be an integer or fraction in the field k and we have $n(\alpha) = \pm n$; Theorem 102 follows when we recall that it holds for $n = -1$.

Thus, using the transcendental methods just developed, we establish the results of Sect. 71 to Sect. 78 in reverse order to that in which they were obtained by the purely arithmetic means we adopted earlier.

§83. Strict Form of the Equivalence and Class Concepts

If we take as basis for our discussions the strict concept of equivalence explained in Sect. 24 the results established in Chapters 17 and 18 require only simple, easily discovered modifications.

First it is clear that the strict equivalence of Sect. 24 coincides with the original concept of equivalence in every imaginary quadratic field k and in every real quadratic field k for which the norm $n(\varepsilon)$ of the fundamental unit is -1. In the case, however, where k is real and $n(\varepsilon) = +1$ each ideal class according to the original definition decomposes into two classes with respect

to the strict form of equivalence; in particular the principal class according to the original definition splits into two classes according to the strict definition, namely the strict classes determined by the principal ideal (1) and by the principal ideal $(\sqrt{m})$. If we denote by h' the number of ideal classes in the strict sense then, under the conditions most recently stated, we have $h' = 2h$ (*Dedekind* (1)).

§84. The Fundamental Theorem for the New Class and Genus Concepts

To the strict notion of class there corresponds a new concept of genus; namely, the genus of an ideal $\mathfrak{i}$ in the field $k(\sqrt{m})$ will be characterized uniformly in all cases by the t units

$$\left(\frac{+n(\mathfrak{i}), m}{l_1}\right), \ldots, \left(\frac{+n(\mathfrak{i}), m}{l_t}\right)$$

where the norm of $\mathfrak{i}$ (in distinction from the earlier definition) always has the positive sign. For an imaginary field k this new notion of genus coincides completely with the old. This is the case also for a real field k provided that the character set of the number -1 in k consists entirely of positive units. This last condition must obviously be satisfied in all cases where the norm of the fundamental unit is -1. Now let k be a real field for which the norm of the fundamental unit is $+1$. There are two cases to consider according as the character set of -1 in k consists entirely of positive units or not.

In the first case the ideals (1) and $(\sqrt{m})$ both belong to the same genus since

$$\left(\frac{n(\mathfrak{a}), m}{l_i}\right) = \left(\frac{+m, m}{l_i}\right) = \left(\frac{+m, m}{l_i}\right)\left(\frac{-1, m}{l_i}\right) = \left(\frac{-m, m}{l_i}\right) = +1$$

for $i = 1, \ldots, t$. The new genera thus consist of the same ideals as the old and the number of genera is again 2^{t-1}.

In the second case the two (strict) ideal classes represented by the ideal (1) and by the ideal $(\sqrt{m})$ belong to different (new) genera. The number of new genera is twice that of the old; in this case the number of individual characters involved in the definition of the original notion of genus was $t-1$ and hence the number of old genera was 2^{t-2}. As a consequence the number of new genera is 2^{t-1}, as in the first case. Further, since in this case we have

$$\left(\frac{-1, m}{l_1}\right) \cdots \left(\frac{-1, m}{l_t}\right) = +1$$

the fundamental Theorem 100 holds for the new concept of equivalence and the new notion of genus when we replace r by t.

The remaining results and proofs of Chapters 17 and 18 can likewise be transformed without difficulty and some of them even take a simpler form when the new notions are used.

19. Determination of the Number of Ideal Classes of a Quadratic Field

§85. The Symbol $\left(\frac{a}{n}\right)$ for a Composite Number n

A remarkable formula for the number h of ideal classes of the quadratic field k results from the expression in Theorem 109 if we evaluate the expression

$$\lim_{s=1} \prod_{(p)} \frac{1}{1-\left(\frac{d}{p}\right)p^{-s}}$$

on the right hand side in closed form. To this end it is necessary to define the symbol $\left(\frac{a}{n}\right)$ also in the case where n is a composite positive rational integer. If $n = pq \ldots w$ where $p, q, \ldots, w$ are rational prime numbers (equal or distinct) then we define

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)\cdots\left(\frac{a}{w}\right);$$

in addition $\left(\frac{a}{1}\right)$ will always be $+1$. In this way we obtain for $s > 1$

$$\prod_{(p)} \frac{1}{1-\left(\frac{d}{p}\right)p^{-s}} = \sum_{(n)} \left(\frac{d}{n}\right) \cdot \frac{1}{n^s},$$

where the sum is taken over all positive rational integers n. Evaluation of the limit of this sum for $s = 1$ leads to a closed form for the class number h; we give the result in the next theorem.

§86. Closed Form for the Number of Ideal Classes

Theorem 114. *The number h of ideal classes of the field $k(\sqrt{m})$ is*

$$h = -\frac{w}{2|d|}\sum_{(n)}\left(\frac{d}{n}\right)n \qquad \text{for } m < 0$$[1]

and

$$h = \frac{1}{2\log\varepsilon}\log\frac{\prod\limits_{(b)}(e^{b\pi i/d} - e^{-b\pi i/d})}{\prod\limits_{(a)}(e^{a\pi i/d} - e^{-a\pi i/d})} \qquad \text{for } m > 1$$

where the sum $\sum\limits_{(n)}$ runs over the $|d|$ rational integers $n = 1, 2, \ldots, |d|$ and the products $\prod\limits_{(a)}$ and $\prod\limits_{(b)}$ over all the numbers a, b among these d integers which satisfy the conditions $\left(\frac{d}{a}\right) = +1$, $\left(\frac{d}{b}\right) = -1$ respectively (Dirichlet (8, 9), Weber (4)).

Proof. Let n, n' be positive integers. If n and d have a common divisor other than ± 1 then $\left(\frac{d}{n}\right) = 0$. On the other hand, if n is relatively prime to d then it is easily seen that $\left(\frac{d}{n}\right) = \prod\limits_{(w)}\left(\frac{d, n}{w}\right)$ where the product runs over all the distinct rational prime numbers w which divide n. According to Lemma 14 the product $\prod\limits_{(l)}\left(\frac{d, n}{l}\right)$ represents the same unit if l runs through all prime factors of d. If now $n' \equiv n \pmod{d}$ we have

$$\prod_{(l)}\left(\frac{d, n}{l}\right) = \prod_{(l)}\left(\frac{d, n'}{l}\right)$$

and hence we obtain

$$\left(\frac{d}{n}\right) = \left(\frac{d}{n'}\right) \tag{19.1}$$

if $n \equiv n' \pmod{d}$.

We deduce further that

$$\left(\frac{d}{1}\right) + \left(\frac{d}{2}\right) + \cdots + \left(\frac{d}{|d|}\right) = 0 \tag{19.2}$$

[1] Hilbert does not make it clear that w in this formula stands for the number of roots of unity in $k(\sqrt{m})$.

if we determine a number b such that $\left(\frac{d}{b}\right) = -1$ and then take into account the fact that the left hand side of (19.2) can be put in the form

$$\left(\frac{d}{b}\right) + \left(\frac{d}{2b}\right) + \cdots + \left(\frac{d}{|d|b}\right) = -\left\{\left(\frac{d}{1}\right) + \left(\frac{d}{2}\right) + \cdots + \left(\frac{d}{|d|}\right)\right\}$$

by the use of (19.1).

Using the formula

$$\frac{1}{n^s} = \frac{1}{\Gamma(s)} \int_0^\infty e^{-nt} t^{s-1} dt$$

and the rule (19.1) we deduce that

$$\lim_{s=1} \sum_{(n)} \left(\frac{d}{n}\right) \cdot \frac{1}{n^s} = \lim_{s=1} \int_0^\infty \frac{F(e^{-t}) t^{s-1}}{1 - e^{-|d|t}} dt$$

where we write $F(x)$ as an abbreviation for

$$\left(\frac{d}{1}\right)x + \left(\frac{d}{2}\right)x^2 + \cdots + \left(\frac{d}{|d|}\right)x^{|d|}.$$

By virtue of equation (19.2) $F(x)$ has the factor $1 - x$; hence the function $\dfrac{F(e^{-t})}{1 - e^{-|d|t}}$, which is rational in e^{-t}, remains finite for $t = 0$. It follows that

$$\lim_{s=1} \int_0^\infty \frac{F(e^{-t}) t^{s-1}}{1 - e^{-|d|t}} dt = \int_0^\infty \frac{F(e^{-t})}{1 - e^{-|d|t}} dt.$$

If we introduce a new variable of integration $x = e^{-t}$ in the latter integral it takes the form

$$\int_0^1 \frac{F(x)}{x(1 - x^{|d|})} dx.$$

Now we have the partial fraction decomposition

$$\frac{F(x)}{x(1 - x^{|d|})} = -\frac{1}{|d|} \sum_{(n)} \frac{F(e^{2\pi i n/|d|})}{x - e^{2\pi i n/|d|}},$$

where the sum is taken over $n = 1, 2, \ldots, |d|$. According to a theorem of Gauss we have

$$F(e^{2\pi i n/|d|}) = \sum_{n'} \left(\frac{d}{n'}\right) e^{2\pi i n n'/|d|} = \left(\frac{d}{n}\right)\sqrt{d}$$

where n' runs through the integers $1, 2, \ldots, |d|$ and $\sqrt{d}$ is positive for positive d and positive imaginary for negative d (cf. Sect. 27.4). Since

$$\int_0^1 \frac{dx}{x - e^{2\pi in/|d|}} = \log \frac{e^{\pi in/|d|} - e^{-\pi in/d}}{i} - \frac{i\pi}{|d|}(n - \frac{1}{2}d)$$

for $n = 1, 2, \ldots, |d|$ (where we take the real value of the logarithm), the result stated in Theorem 114 follows without difficulty.

The form of the result is essentially different according as the field k is imaginary or real. In the first case h can be calculated directly from the given formula. In the second case we need to know first the fundamental unit ε; the quotient of the two products $\prod\limits_{(a)}$ and $\prod\limits_{(b)}$ as will be shown later (in Sect. 27.1) is identical with a certain unit for the quadratic field k derived from the theory of cyclotomic fields.

To take an example for the case of an imaginary field, when $m = -p$ where p is a positive rational prime greater than 3 and congruent to 3 modulo 4, we obtain

$$h = \frac{\sum b - \sum a}{p}$$

where $\sum a$ and $\sum b$ denote respectively the sums of the quadratic residues and non-residues modulo p which lie between 0 and p. By an easy transformation we can eliminate the denominator p in the above expression: the class number h is equal either to the excess of the number of quadratic residues between 0 and $p/2$ over the number of non-residues in the same range or else to one third of this excess according as p is congruent to 7 or 3 modulo 8. The number of residues thus exceeds the number of non-residues, a fact which has not yet been proved by purely arithmetic means.

§87. Dirichlet Biquadratic Number Fields

The following problem is a natural generalisation of the theory of quadratic fields we have developed thus far. Instead of the usual field of rational numbers we take as ground field a quadratic field k; then we study the quadratic extension fields of k, i.e. those biquadratic fields K which include the given field k as subfield.

If k is the field generated by the imaginary unit $\sqrt{-1}$ we call K a *Dirichlet biquadratic field*. Extensive investigations have been made in this case (*Dirichlet* (10, 11, 12), *Eisenstein* (3, 6), *Bachmann* (1, 3), *Minnigerode* (1), *Hilbert* (5)). With a suitable extension of terminology the fundamental Theorem 100 concerning the classification of the ideal classes of K into genera holds in this case also and the two methods of proof of this theorem which were described in Chapter 18 can both be applied to the field K, so that the fundamental theorem for Dirichlet biquadratic fields admits both

a purely arithmetic proof (*Hilbert* (5)) and a proof by means of Dirichlet's transcendental methods (*Dirichlet* (10, 11, 12), *Minnigerode* (1)).

Of particular interest is the case where the Dirichlet biquadratic field K includes not only the quadratic field $k(\sqrt{-1})$ but also two other quadratic fields $k(\sqrt{+m})$ and $k(\sqrt{-m})$. For such a *special Dirichlet field* K we have the following result which may also be proved by both transcendental and purely arithmetic methods.

Theorem 115. *The number of ideal classes in a special Dirichlet biquadratic field $K(\sqrt{+m}, \sqrt{-m})$ is either the product of the class number of the quadratic fields $k(\sqrt{+m})$ and $k(\sqrt{-m})$ or else half this product according as the relative norm of the fundamental unit of K with respect to $k(\sqrt{-1})$ is $\pm i$ or ± 1.*

Dirichlet called this result one of the most beautiful theorems of the theory of imaginary numbers, disclosing as it does a surprising connexion between the quadratic fields generated by the square roots of real numbers of opposite sign.

By means of a purely arithmetic proof of this theorem it is possible also by very simple means to characterize (by certain conditions on the genus characters) which ideal classes of the biquadratic field $K(\sqrt{+m}, \sqrt{-m})$ can be expressed as products of an ideal class of $k(\sqrt{+m})$ and an ideal class of $k(\sqrt{-m})$ (*Hilbert* (5)).

20. Orders and Modules of Quadratic Fields

§88. Orders of a Quadratic Field

The theory of orders and modules in a quadratic field k is quickly settled by specialising the general results developed in Chapter 9. We discover easily that each order r of the field k can be generated by a single number of the form $\rho = f\omega$ where ω is the number defined in Sect. 59 which together with 1 forms a basis for k and f is a certain positive integer, namely the conductor of r. If in particular the discriminant d is negative and actually less than -4 then, according to Theorem 66, the number h_r of regular order classes of the order r is given by the formula

$$h_r = hf \prod_{(p)} \left(1 - \left(\frac{d}{p}\right)\frac{1}{p}\right)$$

where the product is taken over all distinct rational prime numbers p dividing f (*Dedekind* (1, 3)).

§89. Theorem on the Module Classes of a Quadratic Field. Binary Quadratic Forms

In connexion with the module classes of a quadratic field we have the following result.

Theorem 116. *In every module class of a quadratic field k there exist regular order ideals* (*Dedekind* (1)).

Proof. Let $[\mu_1, \mu_2]$ be a module in the field k, where μ_1 and μ_2 are integers; let $\partial = f^2 d$ be the discriminant of the module class determined by $[\mu_1, \mu_2]$; let $\mathfrak{m} = (\mu_1, \mu_2)$ be the ideal generated by μ_1 and μ_2 and $\mathfrak{m}' = s\mathfrak{m}$ the ideal conjugate to $\mathfrak{m}$. Now we fix an integer α of the field k divisible by $\mathfrak{m}'$ such

that $\alpha/\mathfrak{m}'$ is prime to ∂. Then we set

$$\alpha_1 = \frac{\alpha\mu_1}{n(\mathfrak{m})}, \quad \alpha_2 = \frac{\alpha\mu_2}{n(\mathfrak{m})},$$

so that $[\alpha_1, \alpha_2]$ is a module equivalent to $[\mu_1, \mu_2]$ while the ideal $\mathfrak{a} = (\alpha_1, \alpha_2)$ generated by α_1, α_2 is prime to ∂.

If ∂ is an even number we consider first the three integers α_1, α_2, $\alpha_1 + \alpha_2$; at least one of these must be prime to 2 for otherwise we would certainly find some pair of these integers which have exactly the same prime ideal common factor with 2 and this contradicts the fact that the ideal $\mathfrak{a}$ is prime to 2. Denote the odd rational prime numbers dividing ∂ by p, q, $\ldots$, w. Since $\mathfrak{a}$ is prime to p at least one of the three numbers α_1, $\alpha_1 + \alpha_2$, $\alpha_1 + 2\alpha_2$ must be prime to p: say $\alpha_1 + x\alpha_2$ is prime to p and similarly $\alpha_1 + y\alpha_2$ prime to q and so on, where x, y, $\ldots$ are rational integers. We deduce easily that there is a rational integer a such that $\alpha_1 + a\alpha_2$ is prime to ∂.

Now we set

$$b = \frac{|n(\alpha_1 + a\alpha_2)|}{n(\mathfrak{a})}, \quad \beta = \frac{\alpha_2(\alpha_1' + a\alpha_2')}{n(\mathfrak{a})},$$

where α_1', α_2' are the conjugates of α_1, α_2 respectively; b is a positive rational integer and β is an algebraic integer; the module $[\alpha_1, \alpha_2] = [\alpha_1 + a\alpha_2, \alpha_2]$ is equivalent to the module $[b, \beta]$. At the same time, since

$$(b, \beta) = \frac{\alpha_1' + a\alpha_2'}{\mathfrak{a}'},$$

the norm $n(b, \beta) = b$. The module $[b, \beta]$ is obviously a regular order ideal in the order $r = [\beta]$ generated by the number β and hence Theorem 116 is completely proved.

Since

$$\partial = \frac{1}{(n(b,\beta))^2} \begin{vmatrix} b & \beta \\ b & \beta' \end{vmatrix}^2 = \begin{vmatrix} 1 & \beta \\ 1 & \beta' \end{vmatrix}^2$$

the discriminant of this order r coincides with the discriminant of the module class under consideration. The order r we have obtained is also the only one which produces modules equivalent to $[\mu_1, \mu_2]$ among its regular order ideals. Theorem 116 shows that in a quadratic field the study of module classes and of classes of regular order ideals are essentially the same,

According to our general discussion in Sect. 30 and Sect. 35 there corresponds to each module class of a quadratic field $k(\sqrt{m})$ a class of binary quadratic forms with rational integer coefficients and conversely to each such class of forms with non-square discriminant there corresponds a module class of a quadratic field such that the forms and the module class have the same discriminant. Accordingly the theory of quadratic forms with prescribed discriminant ∂ is completely settled by the investigations of this section.

§90. Lower and Higher Theories of Quadratic Fields

The study we have developed and systematically presented in this third part of the Report constitutes the *lower* theory of quadratic number fields. By the *higher* theory of quadratic number fields I understand those properties of such fields for whose natural development it is necessary to use certain auxiliary fields of higher degree. A part of this higher theory is discussed in the fourth part of the Report. The theory of the class field of an imaginary quadratic field and the abelian extensions of such a field, however, requires for its construction the method of complex multiplication of elliptic functions and this is a subject which cannot be included in this Report.

Part IV

Cyclotomic Fields

21. The Roots of Unity with Prime Number Exponent l and the Cyclotomic Field They Generate

§91. Degree of the Cyclotomic Field of the l-th Roots of Unity; Factorisation of the Prime Number l

Let l be an odd rational prime number and let $\zeta = e^{2\pi i/l}$. The l-th degree equation

$$x^l - 1 = 0$$

has the l roots

$$\zeta, \zeta^2, \ldots, \zeta^{l-1}, \zeta^l = 1.$$

These numbers are called the *l-th roots of unity.* The field which they generate is denoted by $k(\zeta)$ and is called the *cyclotomic field of the l-th roots of unity.* This field has the following properties.

Theorem 117. *If l is an odd prime number then the cyclotomic field $k(\zeta)$ of the l-th roots of unity generated by $\zeta = e^{2\pi i/l}$ has degree $l-1$. The prime number l splits in $k(\zeta)$ as $l = \mathfrak{l}^{l-1}$ where $\mathfrak{l} = (1-\zeta)$ is a prime ideal of degree 1 in $k(\zeta)$.*

Proof. The number ζ satisfies the equation

$$F(x) = \frac{x^l - 1}{x - 1} = x^{l-1} + x^{l-2} + \cdots + x + 1 = 0$$

of degree $l-1$; so the degree of the field $k(\zeta)$ is at most $l-1$. Since ζ, ζ^2, ..., ζ^{l-1} are the $l-1$ roots of the equation $F(x) = 0$ we have

$$x^{l-1} + x^{l-2} + \cdots + 1 = (x-\zeta)(x-\zeta^2)\cdots(x-\zeta^{l-1})$$

identically in x; when we put $x = 1$ it follows that

$$l = (1-\zeta)(1-\zeta^2)\cdots(1-\zeta^{l-1}). \tag{21.1}$$

Let g be any rational integer greater than 1 and not divisible by l; there exists a positive rational number g' such that $gg' \equiv 1 \pmod{l}$. Then the quotients

$$\frac{1-\zeta^g}{1-\zeta} = 1 + \zeta + \zeta^2 + \cdots + \zeta^{g-1}$$

and

$$\frac{1-\zeta}{1-\zeta^g} = \frac{1-\zeta^{gg'}}{1-\zeta^g} = \frac{1-(\zeta^g)^{g'}}{1-\zeta^g} = 1+\zeta^g+\zeta^{2g}+\cdots+\zeta^{(g'-1)g}$$

are both algebraic integers and so

$$\varepsilon_g = \frac{1-\zeta^g}{1-\zeta}$$

is a unit of the field $k(\zeta)$. If we set $\lambda = 1-\zeta$ and $\mathfrak{l} = (\lambda)$ then formula (21.1) takes the form

$$l = \lambda^{l-1}\varepsilon_2\varepsilon_3\cdots\varepsilon_{l-1} = \mathfrak{l}^{l-1}. \tag{21.2}$$

We deduce immediately from Theorem 33 that in a given number field the number of prime ideal factors of a rational prime number cannot exceed the degree of the field. It follows from equation (21.2) that the degree of $k(\zeta)$ must be at least $l-1$; hence, in view of our earlier remarks, this degree is precisely $l-1$. Furthermore we deduce from the same result that the ideal $\mathfrak{l}$ in $k(\zeta)$ cannot split into further factors and hence $\mathfrak{l}$ is a prime ideal of $k(\zeta)$ (*Dedekind* (1)).

The result we have obtained shows at the same time that the polynomial $F(x)$ is irreducible in the field of rational numbers.

§92. Basis and Discriminant of the Cyclotomic Field of the l-th Roots of Unity

Theorem 118. *In the cyclotomic field $k(\zeta)$ of the l-th roots of unity generated by $\zeta = e^{2\pi i/l}$ the numbers*

$$1, \zeta, \zeta^2, \ldots, \zeta^{l-2}$$

form a basis. The discriminant of the cyclotomic field $k(\zeta)$ is

$$d = (-1)^{\frac{1}{2}(l-1)} l^{l-2}.$$

Proof. The different of the number ζ in the field $k(\zeta)$ is

$$\delta = (\zeta-\zeta^2)(\zeta-\zeta^3)\cdots(\zeta-\zeta^{l-1}) = \left[\frac{dF(x)}{dx}\right]_{x=\zeta}.$$

Since

$$(x-1)F(x) = x^l - 1$$

we have

$$(x-1)\frac{dF(x)}{dx} + F(x) = lx^{l-1}$$

and hence

$$\delta = -\frac{l\zeta^{l-1}}{1-\zeta}.$$

According to a remark we made in Sect. 3 (p. 5) it follows that the discriminant of the number ζ is

$$d(\zeta) = (-1)^{\frac{1}{2}(l-1)(l-2)} n(\delta) = (-1)^{\frac{1}{2}(l-1)} l^{l-2}.$$

Since the discriminant $d(\lambda)$ of the number λ clearly has the same value $d(\zeta)$ we deduce from the discussion in the proof of Theorem 5 near the formula [illegible]

$$\alpha = \frac{a_0 + a_1\lambda + \cdots + a_{l-2}\lambda^{l-2}}{l^{l-2}} \tag{21.3}$$

with rational integer coefficients $a_0, a_1, \ldots, a_{l-2}$.

We claim that these numbers $a_0, a_1, \ldots, a_{l-2}$ must all be divisible by l^{l-2}. We show first that they are all divisible by l, as follows. If this were not the case we let a_g be the first among them which is not divisible by l. Since $l^{l-2}\alpha \equiv 0 \pmod{l}$ and $l = \mathfrak{l}^{l-1}$ we would have $a_g\lambda^g \equiv 0 \pmod{\mathfrak{l}^{g+1}}$ whence $a_g \equiv 0 \pmod{\mathfrak{l}}$ and so also $a_g \equiv 0 \pmod{l}$ which is a contradiction. Thus we can cancel one factor l from the numerator and denominator of the expression (21.3). By repetition of this procedure we see finally that for every integer α of the field $k(\zeta)$ the rational coefficients $a_0, a_1, \ldots, a_{l-2}$ and $b_0, b_1, \ldots, b_{l-2}$ in its representations as

$$\alpha = a_0 + a_1\lambda + \cdots + a_{l-2}\lambda^{l-2} = b_0 + b_1\zeta + \cdots + b_{l-2}\zeta^{l-2}$$

are actually all rational integers.

The powers $1, \zeta, \ldots, \zeta^{l-2}$ of the number ζ thus form a basis for the field $k(\zeta)$ and it follows that the discriminant $d(\zeta)$ of the number ζ is at the same time also the discriminant of the field $k(\zeta)$.

§93. Factorisation of the Rational Primes Distinct from l in the Cyclotomic Field of the l-th Roots of Unity

The factorisation of the prime number l in the field $k(\zeta)$ has been described in Theorem 117. For the factorisation in $k(\zeta)$ of the remaining rational prime numbers we have the following rule.

Theorem 119. *Let p be a rational prime number distinct from l; let f be the least positive exponent for which we have $p^f \equiv 1 \pmod{l}$; let $e = (l-1)/f$. Then in the cyclotomic field $k(\zeta)$ we have the factorisation*

$$p = \mathfrak{p}_1 \cdots \mathfrak{p}_e$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_e$ are distinct prime ideals of degree f in $k(\zeta)$ (*Kummer* (5, 6)).

Proof. Let $\alpha = a + a_1\zeta + \cdots + a_{l-2}\zeta^{l-2}$ be any integer of the cyclotomic field $k(\zeta)$. Then we have the congruences

$$\begin{aligned}
\alpha^p &\equiv (a + a_1\zeta + \cdots + a_{l-2}\zeta^{l-2})^p \equiv a + a_1\zeta^p + \cdots + a_{l-2}\zeta^{p(l-2)} \\
\alpha^{p^2} &\equiv (a + a_1\zeta^p + \cdots + a_{l-2}\zeta^{p(l-2)})^p \equiv a + a_1\zeta^{p^2} + \cdots + a_{l-2}\zeta^{p^2(l-2)} \\
&\cdots\cdots\cdots \\
\alpha^{p^f} &\equiv (a + a_1\zeta^{p^{f-1}} + \cdots + a_{l-2}\zeta^{p^{f-1}(l-2)})^p \\
&\equiv a + a_1\zeta^{p^f} + \cdots + a_{l-2}\zeta^{p^f(l-2)} \equiv \alpha
\end{aligned}$$

all modulo p. If $\mathfrak{p}$ is any prime ideal of $k(\zeta)$ which divides p then, from the congruence $\alpha^{p^f} \equiv \alpha \pmod{p}$ which we have just obtained we have *a fortiori* that $\alpha^{p^f} \equiv \alpha \pmod{\mathfrak{p}}$. Thus the congruence

$$\xi^{p^f} - \xi \equiv 0 \pmod{\mathfrak{p}} \tag{21.4}$$

is satisfied by every integer of the field $k(\zeta)$. The number of roots of this congruence which are mutually incongruent modulo $\mathfrak{p}$ is thus equal to the number of integers mutually incongruent modulo $\mathfrak{p}$, and this is $n(\mathfrak{p}) = p^{f'}$ where f' is the degree of the prime ideal $\mathfrak{p}$. Now the degree of the congruence (21.4) is p^f; so it follows from Theorem 26 that $p^{f'} \le p^f$ and so $f' \le f$.

On the other hand, according to Theorem 24, the generalised Fermat Theorem, we have

$$\zeta^{p^{f'}-1} \equiv 1 \pmod{\mathfrak{p}}. \tag{21.5}$$

Since, according to (21.1), the number $1 - \zeta^g$ is prime to $\mathfrak{p}$ for all exponents g prime to l, it follows from the congruence (21.5) that $p^{f'} - 1 \equiv 0 \pmod{l}$ and hence that $f' \ge f$. We conclude at once that $f' = f$; so each prime ideal which divides p has degree f.

Since p does not divide the discriminant of the field $k(\zeta)$ it follows from Theorem 31 that p splits as a product of distinct prime ideals. Suppose we have $p = \mathfrak{p}_1 \cdots \mathfrak{p}_{e'}$; then $n(p) = p^{l-1} = p^{e'f}$, whence $l - 1 = e'f$ and so $e' = (l-1)/f = e$. This completes the proof of Theorem 119.

For the actual determination of the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_e$ we apply Theorem 33 and take into account the remark relating to it on p. 31, according to which there exists a factorisation

$$F(x) \equiv F_1(x) \dots F_e(x) \pmod{p}$$

identically in x, where $F_1(x), \dots, F_e(x)$ are polynomials of degree f in x with rational integer coefficients which are irreducible and mutually incongruent modulo p. Once we have determined these polynomials we obtain the desired representation in the following formulæ:

$$\mathfrak{p}_1 = (p, F_1(\zeta)), \dots, \mathfrak{p}_e = (p, F_e(\zeta)).$$

22. The Roots of Unity for a Composite Exponent m and the Cyclotomic Field They Generate

§94. The Cyclotomic Field of the m-th Roots of Unity

Let m be an arbitrary positive rational integer; set $\mathsf{Z} = e^{2\pi i/m}$. The m-th degree equation

$$x^m - 1 = 0$$

has the m roots

$$\mathsf{Z}, \mathsf{Z}^2, \ldots, \mathsf{Z}^{m-1}, \mathsf{Z}^m = 1.$$

These numbers are called the m-th *roots of unity*; the field which they generate is denoted by $k(\mathsf{Z})$ and is called the *cyclotomic field of the m-th roots of unity.*

If m is divisible by more than one prime number we set

$$m = l_1^{h_1} l_2^{h_2} \cdots$$

where l_1, l_2, ... are distinct rational primes. Then we can construct a partial fraction decomposition

$$\frac{1}{m} = \frac{a_1}{l_1^{h_1}} + \frac{a_2}{l_2^{h_2}} + \cdots$$

where a_1, a_2, ... are positive or negative rational integers and a_1 is prime to l_1, a_2 to l_2, ... Using this decomposition we obtain the factorisation

$$\mathsf{Z} = \mathsf{Z}_1^{a_1} \mathsf{Z}_2^{a_2} \cdots$$

where $\mathsf{Z}_1 = e^{2\pi i/l_1^{h_1}}$, $\mathsf{Z}_2 = e^{2\pi i/l_2^{h_2}}$, ... Thus the compositum of the field $k(\mathsf{Z}_1)$ of the $l_1^{h_1}$-th roots of unity, the field $k(\mathsf{Z}_2)$ of the $l_2^{h_2}$-th roots of unity, ... is precisely the field $k(\mathsf{Z})$. Accordingly we study first the simpler case $m = l^h$ where m has only one prime factor l.

§95. Degree of the Cyclotomic Field of the l^h-th Roots of Unity and the Factorisation of the Prime Number l in This Field

For the cyclotomic field of the l^h-th roots of unity we have the following results.

Theorem 120. *Let l be any prime number (even or odd). Then the cyclotomic field $k(\mathsf{Z})$ of the l^h-th roots of unity generated by $\mathsf{Z} = e^{2\pi i/l^h}$ has degree $l^h(l-1)$. In $k(\mathsf{Z})$ the prime number l splits as $l = \mathfrak{L}^{l^{h-1}(l-1)}$ where $\mathfrak{L}$ is a prime ideal of degree 1 in $k(\mathsf{Z})$.*

Proof. Z satisfies the equation

$$F(x) = \frac{x^{l^h} - 1}{x^{l^{h-1}} - 1} = x^{l^{h-1}(l-1)} + x^{l^{h-1}(l-2)} + \cdots + 1 = 0$$

of degree $l^{h-1}(l-1)$. If g is a rational integer not divisible by l and g' is a rational integer such that $gg' \equiv 1 \pmod{l^h}$ then, just as on p. 162, we deduce that both

$$\mathsf{E}_g = \frac{1 - \mathsf{Z}^g}{1 - \mathsf{Z}}$$

and also its reciprocal

$$\frac{1 - \mathsf{Z}}{1 - \mathsf{Z}^g} = \frac{1 - \mathsf{Z}^{gg'}}{1 - \mathsf{Z}^g}$$

are integers; hence E_g is a unit. From this observation we can deduce, just as in Sect. 91, that

$$F(1) = l = \prod_{(g)}(1 - \mathsf{Z}^g) = \Lambda^{l^{h-1}(l-1)} \prod_{(g)} \mathsf{E}_g = \mathfrak{L}^{l^{h-1}(l-1)}$$

where $\Lambda = 1 - \mathsf{Z}$, $\mathfrak{L} = (\Lambda)$ and in the product g runs over all integers prime to l greater than 0 and less than l^h.

Using the same line of argument as in Sect. 91 we deduce that the degree of the field $k(\mathsf{Z})$ is at least $l^{h-1}(l-1)$ and hence that it has precisely this value.

§96. Basis and Discriminant of the Cyclotomic Field of the l^h-th Roots of Unity

Theorem 121. *In the cyclotomic field $k(\mathsf{Z})$ of the l^h-th roots of unity generated by $\mathsf{Z} = e^{2\pi i/l^h}$ the numbers*

$$1, \mathsf{Z}, \mathsf{Z}^2, \ldots, \mathsf{Z}^{l^{h-1}(l-1)-1}$$

form a basis. The discriminant of this field is

$$d = \pm l^{l^{h-1}(hl-h-1)}$$

where for $l^h = 4$ or $l \equiv 3 \pmod 4$ the negative sign is taken and otherwise the sign is positive.

Theorem 122. *Let p be a rational prime number distinct from l. Let f be the least positive exponent for which $p^f \equiv 1 \pmod{l^h}$; let $e = l^{h-1}(l-1)/f$. Then p splits in the cyclotomic field $k(\mathsf{Z})$ as*

$$p = \mathfrak{P}_1 \cdots \mathfrak{P}_e$$

where $\mathfrak{P}_1, \ldots, \mathfrak{P}_e$ are distinct prime ideals of degree f in $K(\mathsf{Z})$.

Theorems 121 and 122 are proved in exactly the same way as the corresponding Theorems 118 and 119 for the field $k(\zeta)$.

§97. The Cyclotomic Field of the m-th Roots of Unity. Degree, Discriminant and Prime Ideals of This Field

Now let m be a product of powers of distinct prime numbers, say $m = l_1^{h_1} l_2^{h_2} \cdots$. The cyclotomic field $k(\mathsf{Z})$ of the m-th roots of unity defined in Sect. 94 is formed (as we showed there) by composing the cyclotomic fields $k(\mathsf{Z}_1)$, $k(\mathsf{Z}_2)$, ... of the $l_1^{h_1}$-th, $l_2^{h_2}$-th, roots of unity. Since the discriminants of these latter cyclotomic fields are all prime to one another we have the following result as an immediate consequence of Theorem 87 (Sect. 52).

Theorem 123. *Let $m = l_1^{h_1} l_2^{h_2} \cdots$; the degree of the cyclotomic field $k(\mathsf{Z})$ of the m-th roots of unity is*

$$\Phi(m) = l_1^{h_1-1}(l_1-1) l_2^{h_2-1}(l_2-1) \cdots .$$

If we apply the second assertion in Theorem 88 to the cyclotomic fields $k(\mathsf{Z}_1)$, $k(\mathsf{Z}_2)$, ..., taking into account Theorem 121, we obtain the further statement.

Theorem 124. *The cyclotomic field $k(\mathsf{Z})$ of the m-th roots of unity has as basis the numbers $1, \mathsf{Z}, \mathsf{Z}^2, \ldots, \mathsf{Z}^{\Phi(m)-1}$.*

The discriminant of $k(\mathsf{Z})$ can be deduced from the first assertion of Theorem 88.

Finally, on the basis of Theorem 88, with the aid of the properties of the decomposition and inertia fields, we can determine the factorisation of a rational prime number p in the field $k(\mathsf{Z})$. We have the following result.

Theorem 125. *Let p be a rational prime number p which does not divide $m = l_1^{h_1} l_2^{h_2} \cdots$. Let f be the least positive exponent for which $p^f \equiv 1 \pmod{m}$; let $e = \Phi(m)/f$. Then p splits in the cyclotomic field $k(\mathsf{Z})$ of the m-th roots of unity as*

$$p = \mathfrak{P}_1 \cdots \mathfrak{P}_e$$

where $\mathfrak{P}_1, \ldots, \mathfrak{P}_e$ are distinct prime ideals of degree f in $k(\mathsf{Z})$.

If p^h is a power of p and $m^* = p^h m$ then in the cyclotomic field $k(\mathsf{Z}^*)$ of the m^*-th roots of unity we have the factorisation

$$p = \{\mathfrak{P}_1^* \cdots \mathfrak{P}_e^*\}^{p^{h-1}(p-1)}$$

where $\mathfrak{P}_1^*, \ldots, \mathfrak{P}_e^*$ are distinct prime ideals of degree f in $k(\mathsf{Z}^*)$ (Kummer (15), Dedekind (5), Weber (4)).

In the proof of Theorem 125 we take (for the sake of brevity) $m = l_1^{h_1} l_2^{h_2}$ and denote the cyclotomic fields of the $l_1^{h_1}$-th and $l_2^{h_2}$-th roots of unity by $k^{(1)}$ and $k^{(2)}$ respectively. Let p be a rational prime number distinct from l_1 and l_2 and let $\mathfrak{p}^{(1)}, \mathfrak{p}^{(2)}$ be prime ideal factors of p in $k^{(1)}, k^{(2)}$ respectively. We denote the decomposition fields of $\mathfrak{p}^{(1)}$, $\mathfrak{p}^{(2)}$ in $k^{(1)}$, $k^{(2)}$ by $k_z^{(1)}$, $k_z^{(2)}$respectively. Let f_1, f_2 be the least exponents for which we have $p^{f_1} \equiv 1 \pmod{l_1^{h_1}}$, $p^{f_2} \equiv 1 \pmod{l_2^{h_2}}$ respectively. Set

$$e_1 = l_1^{h_1-1}(l_1 - 1)/f_1 \quad \text{and} \quad e_2 = l_2^{h_2-1}(l_2 - 1)/f_2.$$

Then e_1 and e_2 are the degrees of the fields $k_z^{(1)}$, $k_z^{(2)}$ respectively and f_1, f_2 are the relative degrees of $k^{(1)}$ with respect to $k_z^{(1)}$ and $k^{(2)}$ with respect to $k_z^{(2)}$ respectively. According to Theorem 88 the rational prime number p splits in the compositum $k_z^{(1,2)}$ of $k_z^{(1)}$ and $k_z^{(2)}$ as a product of $e_1 e_2$ ideals which are all prime ideals of degree 1 in $k_z^{(1,2)}$. Among these we consider in particular the prime ideal $\mathfrak{p} = (\mathfrak{p}^{(1)}, \mathfrak{p}^{(2)})$ and denote by $\mathfrak{P}$ a prime factor of $\mathfrak{p}$ in the compositum k of $k^{(1)}$ and $k^{(2)}$; let k_z be the decomposition field of $\mathfrak{P}$ in k. It follows from the definition of decomposition fields that $k_z^{(1,2)}$ either coincides with k_z or else is a subfield of k_z. The group of the compositum of $k^{(1)}$ and $k_z^{(2)}$ over $k_z^{(1,2)}$ is cyclic of degree f_1; the group of the compositum of $k_z^{(1)}$ and $k^{(2)}$ over $k_z^{(1,2)}$ is cyclic of degree f_2. We conclude from this that if f is the least common multiple of f_1 and f_2 then the group of k over $k_z^{(1,2)}$ can have no cyclic subgroup of order greater than f. Since k, being the inertia field of the prime ideal $\mathfrak{P}$, must have a cyclic group over k_z and k_z includes the field $k_z^{(1,2)}$ it follows that the cyclic group of k over k_z has order no greater than f.

On the other hand we introduce the following considerations. The two fields $k^{(1)}$ and k_z have the field $k_z^{(1)}$ but no field of higher degree as common subfield, for otherwise $\mathfrak{p}^{(1)}$ would have to decompose further in $k^{(1)}$. Similarly the fields $k^{(2)}$ and k_z have $k_z^{(2)}$ as greatest common subfield. Now

we take $k_z^{(1,2)}$ as ground field; then k_z is an extension of $k_z^{(1,2)}$ such that no extension of $k_z^{(1,2)}$ included in k_z is included in $k^{(1)}$ or $k^{(2)}$. From this we deduce easily that the relative degree of k_z over $k_z^{(1,2)}$ is at most $f_1 f_2/f$. The degree of k_z is thus at most $e_1 f_1 e_2 f_2/f$ and so the group of k over k_z has order at least f. Taken together with the result proved above, this shows that the order of the group of k over k_z is exactly f. This coincides with the assertion of Theorem 125 in the special case we have been considering.

According to Theorem 123 the number $Z = e^{2\pi i/m}$ satisfies an irreducible equation $F(x) = 0$ of degree $\Phi(m)$ with rational integer coefficients and according to the proof of Theorem 87 this equation $F(x) = 0$ remains irreducible over any field whose discriminant is prime to m (*Kronecker* (3, 21)).

The left hand side $F(x)$ of this equation is formed as follows. If for a moment we use $[m]$ as an abbreviation for $x^m - 1$ and set

$$\begin{aligned}
\Pi_0 &= [m], \\
\Pi_1 &= \left[\frac{m}{l_1}\right]\left[\frac{m}{l_2}\right]\cdots, \\
\Pi_2 &= \left[\frac{m}{l_1 l_2}\right]\left[\frac{m}{l_1 l_3}\right]\cdots\left[\frac{m}{l_2 l_3}\right]\cdots, \\
\Pi_3 &= \left[\frac{m}{l_1 l_2 l_3}\right]\left[\frac{m}{l_1 l_2 l_4}\right]\cdots\left[\frac{m}{l_2 l_3 l_4}\right]\cdots, \\
&\cdots\cdots\cdots
\end{aligned}$$

then

$$F(x) = \frac{\Pi_0 \Pi_2 \Pi_4 \cdots}{\Pi_1 \Pi_3 \Pi_5 \cdots}$$

(*Dedekind* (1), *Bachmann* (2)).

If a is a rational integer and p a prime number not dividing m which divides $F(a)$, then, according to Theorem 125, p satisfies the congruence $p \equiv 1 \pmod{m}$. So there are clearly infinitely many primes p with this property.

§98. Units of the Cyclotomic Field $k(e^{2\pi i/m})$. Definition of the Cyclotomic Units

We have the following results.

Theorem 126. *If m is a power of a prime number l and g is an integer not divisible by l then the expression*

$$\frac{1 - Z^g}{1 - Z}$$

represents a unit in the cyclotomic field generated by $Z = e^{2\pi i/m}$.

If m has more than one prime factor and g is an integer prime to m then the expression

$$1 - Z^g$$

represents a unit in the cyclotomic field generated by $Z = e^{2\pi i/m}$.

Proof. The first statement of this theorem has already been established in the proofs of Theorems 117 and 120. To prove the second part, set $m = l_1^{h_1} l_2^{h_2} l_3^{h_3} \cdots$ and

$$\frac{g}{m} = \frac{a}{l_1^{h_1}} + \frac{b}{l_2^{h_2} l_3^{h_3} \ldots}$$

where a is a rational integer relatively prime to l_1 and b is a rational integer relatively prime to l_2, l_3, ... Then

$$1 - Z^g = 1 - e^{2\pi i g/m} = 1 - e^{(2\pi i a/l_1^{h_1})} e^{(2\pi i b/l_2^{h_2} l_3^{h_3} \cdots)}. \tag{22.1}$$

Now we have

$$\prod_{(x)} \left(1 - e^{(2\pi i x/l_1^{h_1})} e^{(2\pi i b/l_2^{h_2} l_3^{h_3} \cdots)}\right) = 1 - e^{2\pi i b l_1^{h_1}/l_2^{h_2} l_3^{h_3} \cdots},$$

where the product is taken over $x = 0, 1, 2, \ldots, l_1^{h_1} - 1$, or

$$\prod_{(x')} \left(1 - e^{(2\pi i x'/l_1^{h_1})} e^{(2\pi i b/l_2^{h_2} l_3^{h_3} \cdots)}\right) = \frac{1 - e^{2\pi i b l_1^{h_1}/l_2^{h_2} l_3^{h_3} \cdots}}{1 - e^{2\pi i b/l_2^{h_2} l_3^{h_3} \cdots}}. \tag{22.2}$$

where the product is taken over $x' = 1, 2, \ldots, l_1^{h_1} - 1$.

Now we distinguish two cases, according as the number of distinct prime factors l_1, l_2, ... of m is 2 or more than 2. In the first case the right hand side of the formula (22.2) is a unit according to the first part of Theorem 126. In the second case we proceed inductively, supposing that the conclusion of Theorem 126 holds for all cyclotomic fields $k(e^{2\pi i/m^*})$ for which the number m^* has fewer distinct prime factors than has m. Under this hypothesis the theorem holds for the cyclotomic field determined by the $m/l_1^{h_1}$-th roots of unity. Hence the numerator and denominator of the fraction on the right hand side of (22.2) are units. The expression (22.1) is a factor of the product on the left of (22.2) and hence is likewise a unit. Thus Theorem 126 is completely established.

Every unit of a cyclotomic field $k(e^{2\pi i/m})$ has the property that it is equal to the product of a root of unity and a real unit. The root of unity here does not always lie in the field $k(e^{2\pi i/m})$ but may, when m has more than one prime factor, be a $2m$-th or a $4m$-th root of unity according as m is even or odd (*Kronecker* (7)). We state the following result (already known to Kummer).

Theorem 127. *Let l be an odd prime number and in the cyclotomic field $k(\zeta)$ generated by $\zeta = e^{2\pi i/l}$ consider the real subfield $k(\zeta + \zeta^{-1})$ of degree $\frac{1}{2}(l-1)$ generated by $\zeta + \zeta^{-1}$. Then each fundamental set of units for this real subfield $k(\zeta + \zeta^{-1})$ is also a fundamental set of units for $k(\zeta)$.*

Proof. Let $\varepsilon(\zeta)$ be any unit in $k(\zeta)$. Then $\varepsilon(\zeta)/\varepsilon(\zeta^{-1})$ is a unit with the property that all its conjugates have absolute value 1; it follows from Theorem 48 that it is a root of unity. We set $\varepsilon(\zeta)/\varepsilon(\zeta^{-1}) = \pm\zeta^{2g}$ where g is an integer. Then the unit $\eta(\zeta) = \varepsilon(\zeta)\zeta^{-g}$ has the property that

$$\frac{\eta(\zeta)}{\eta(\zeta^{-1})} = \pm 1. \tag{22.3}$$

We assert that in this formula (22.3) the sign on the right hand side must be positive. If it were negative then $\eta(\zeta)$ would be a purely imaginary unit. In this case we set $\eta^2 = \vartheta$; then ϑ would be a unit of the real subfield $k(\zeta+\zeta^{-1})$. The relative different of the number $\eta = \sqrt{\vartheta}$ with respect to $k(\zeta + \zeta^{-1})$ is 2η and hence is prime to l. Accordingly the relative different of the field $k(\zeta)$ with respect to $k(\zeta+\zeta^{-1})$ must also be prime to l. Let $\mathfrak{l}^*$ be any prime ideal of $k(\zeta+\zeta^{-1})$ which divides l; then, according to Theorem 93, this ideal is not equal to the square of a prime ideal of the field $k(\zeta)$. Since, however, $\mathfrak{l}^*$ occurs in l to at most the $\frac{1}{2}(l-1)$-th power, this last conclusion is a contradiction to Theorem 117 concerning the factorisation of the prime number l in the field $k(\zeta)$. Hence on the right hand side of (22.3) we must take the positive sign, i.e. $\eta(\zeta) = \eta(\zeta^{-1})$. It follows that the number $\eta(\zeta)$ is real.

This completes the proof of Theorem 127.

The units given in Theorem 126 are imaginary. In order to obtain real units we form the expressions

$$\mathsf{E}_g = \sqrt{\frac{(1-\mathsf{Z}^g)(1-\mathsf{Z}^{-g})}{(1-\mathsf{Z})(1-\mathsf{Z}^{-1})}}$$

or

$$\mathsf{E}_g = \sqrt{(1-\mathsf{Z}^g)(1-\mathsf{Z}^{-g})}$$

according as m is a power of a single prime or a product of distinct primes. (Here g is an integer prime to m and the positive square roots are taken.) These units are called *cyclotomic units* for short. Referring to the equation $1 - \mathsf{Z}^{-g} = -\mathsf{Z}^{-g}(1-\mathsf{Z}^g)$ we see that in the first case these units lie in the field $k(\mathsf{Z})$ itself while in the second case they appear as products of units of the field $k(\mathsf{Z})$ by $2m$-th or $4m$-th roots of unity according as m is even or odd.

23. Cyclotomic Fields as Abelian Fields

§99. The Group of the Cyclotomic Field of the m-th Roots of Unity

For each positive integer m the cyclotomic field of the m-th roots of unity is easily seen to be an abelian field and indeed we have the following more detailed results.

Theorem 128. *If l is an odd prime number the cyclotomic field generated by $\mathsf{Z} = e^{2\pi i/l^h}$ is a cyclic field.*

The cyclotomic field generated by $\mathsf{Z} = e^{\pi i/2^h}$ $(h \geq 2)$ is obtained by composing the imaginary quadratic field $k(i)$ and the real field $k(e^{\pi i/2^h} + e^{-\pi i/2^h})$. The real field $k(e^{\pi i/2^h} + e^{-\pi i/2^h})$ is cyclic of degree 2^{h-1}.

Proof. We obtain the first part of Theorem 128 if we introduce the automorphism

$$s = (\mathsf{Z} : \mathsf{Z}^r)$$

(replacement of Z by Z^r) where r is a primitive root modulo l^h. Obviously all the automorphisms in the group of the field $k(\mathsf{Z})$ are powers of s.

To prove the second part of Theorem 128 we consider the automorphisms

$$s = (\mathsf{Z} : \mathsf{Z}^5) \quad \text{and} \quad s' = (\mathsf{Z} : \mathsf{Z}^{-1}) = (i : -i).$$

Then it follows easily that all the automorphisms in the group of $k(\mathsf{Z})$ are either powers of s or products of powers of s with s'.

On the basis of Theorem 128 the group of the cyclotomic field of the m-th roots of unity can be immediately obtained for every composite number m.

The decomposition, inertia and ramification fields for a given prime ideal in $k(e^{2\pi i/m})$ are easily determined from the definitions of these fields with the help of the theorems on the decomposition of rational prime numbers in cyclotomic fields which we proved in Sect. 95-97. We have in particular the following result.

Theorem 129. *Let l be an odd prime number and consider the cyclotomic field $k(\mathsf{Z})$ of the l^h-th roots of unity. Then the prime ideal $\mathfrak{L} = (1 - \mathsf{Z})$ of $k(\mathsf{Z})$ which divides l has $k(\mathsf{Z})$ as higher ramification field and the field of l-th roots of unity included in $k(\mathsf{Z})$ as ramification field; the field of rational numbers is both inertia field and decomposition field for $\mathfrak{L}$. If $\mathfrak{P} \neq \mathfrak{L}$ is a prime ideal of $k(\mathsf{Z})$ of degree f then $k(\mathsf{Z})$ is itself the inertia field for $\mathfrak{P}$ while the decomposition field of $\mathfrak{P}$ is the subfield of $k(\mathsf{Z})$ of degree $l^{h-1}(l-1)/f$ belonging to the subgroup consisting of the automorphisms*

$$s^e, s^{2e}, s^{3e}, \ldots, s^{fe}$$

where $s = (\mathsf{Z} : \mathsf{Z}^r)$ is an automorphism of $k(\mathsf{Z})$ which generates its group.

§100. The General Notion of Cyclotomic Field. The Fundamental Theorem on Abelian Fields

We now extend the notion of *cyclotomic field*; we shall understand by a cyclotomic field *simpliciter* not only a field $k(e^{2\pi i/m})$ generated by the roots of unity with a particular exponent m but also any subfield of such a special cyclotomic field $k(e^{2\pi i/m})$. Since each field $k(e^{2\pi i/m})$ is an abelian field and since, further, if m and m' are any exponents, the field of the m-th roots of unity and the field of the m'-th roots of unity are both included as subfields in the field of the mm'-th roots of unity, we have the following general results for the extended notion of cyclotomic field.

Theorem 130. *Every cyclotomic field is an abelian field. Every subfield of a cyclotomic field is a cyclotomic field. Every field formed by the composition of cyclotomic fields is again a cyclotomic field.*

We now have a fundamental result, namely that the first assertion of Theorem 130 has a converse, as follows.

Theorem 131. *Every number field which is an abelian extension of the rational number field is a cyclotomic field* (*Kronecker* (2, 13), *Weber* (1), *Hilbert* (6)).

In preparation for the proof of this fundamental theorem we recall to mind that, according to Sect. 48, every abelian field is composed of cyclic fields for which the degree is a prime number or a power of a prime number. We construct now the following special cyclic fields. Let u be an odd prime number and u^h a power of u with positive exponent; then the field $k(e^{2\pi i/u^{h+1}})$ generated by $e^{2\pi i/u^{h+1}}$ is a cyclic field of degree $u^h(u-1)$. We denote by U_h the cyclic subfield of this field with degree u^h. Next, the number $e^{\pi i/2^{h+1}} + e^{-\pi i/2^{h+1}}$ generates a real cyclic field of degree 2^h. We denote this

field by II_h. Finally, let l^h be a power of any prime number l (even or odd) and p any prime number such that $p \equiv 1 \pmod{l^h}$; then the cyclotomic field $k(e^{2\pi i/p})$ of degree $p-1$ obviously has a cyclic subfield of degree l^h. This cyclic field of degree l^h will be denoted by P_h. The fields U_h, II_h and P_h are cyclotomic fields of degree u^h, 2^h and l^h respectively; according to Theorems 39 and 121 the discriminants of these fields U_h, II_h and P_h are powers of the primes u, 2 and p respectively. It was established in the last remark in Sect. 97 that for every choice of l^h there are prime numbers p with the property that $p \equiv 1 \pmod{l^h}$; this, however, is not in question here.

In the following sections we shall show that every abelian field is a subfield of a field obtained by the composition of $k(i)$ and suitable fields U_h, II_h and P_h. For this proof we first introduce some auxiliary considerations.

§101. A General Lemma on Cyclic Fields

Lemma 15. *Let C_h be a cyclic field of degree l^h where l is a prime number (even or odd). If C_h does not include as a subfield the corresponding field U_1 or II_1 then the compositum of C_h with the field $k(Z)$ generated by $Z = e^{2\pi i/l^h}$ is a field $k(Z, C_h)$ of degree $l^{2h-1}(l-1)$ and there exists an integer κ in $k(Z)$ such that $k(Z, C_h)$ is generated by the numbers Z and $\sqrt[l^h]{\kappa}$; further, if r is any rational integer not divisible by l and $s = (Z : Z^r)$ the corresponding automorphism of $k(Z)$, then κ^{s-r} is the l^h-th power of a number in $k(Z)$.*

Proof. The first assertion of the lemma (concerning the degree of $k(Z, C_h)$) follows at once from the fact that $k(Z)$ and C_h have no subfield in common other than the rational number field. Let α be an integer which generates C_h such that no power of α lies in any subfield of C_h; let t be an automorphism of C_h which generates the group of C_h. For arbitrary exponents a and b we set

$$K(\alpha^a, Z^b) = \alpha^a + Z^b \cdot (t\alpha)^a + Z^{2b} \cdot (t^2\alpha)^a + \cdots + Z^{(l^h-1)b} \cdot (t^{l^h-1}\alpha)^a.$$

The expressions $K(\alpha, Z)$, $K(\alpha^2, Z)$, ..., $K(\alpha^{l^h-1}, Z)$ cannot all vanish for, if they did, then, since $K(\alpha^0, Z) = 0$, the determinant

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ \alpha & t\alpha & \dots & t^{l^h-1}\alpha \\ & & \dots\dots & \\ \alpha^{l^h-1} & (t\alpha)^{l^h-1} & \dots & (t^{l^h-1}\alpha)^{l^h-1} \end{vmatrix}$$

would be zero and hence, according to the remark on p. 6, α would not be a generator of the field C_h. Let $\alpha^* = \alpha^a$ be a power of α for which $K = K(\alpha^*, Z) \neq 0$. Since $K(t\alpha^*, Z^b) = Z^{-b}K(\alpha^*, Z^b)$ it follows that the

number K^{l^h} and hence all the numbers $K(\alpha^*, \mathsf{Z}^b)/K^b$ lie in the field $k(\mathsf{Z})$. Since

$$\alpha^* = \frac{1}{l^h}\{K(\alpha^*, \mathsf{Z}) + K(\alpha^*, \mathsf{Z}^2) + \cdots + K(\alpha^*, \mathsf{Z}^{l^h})\}$$

and α^* is a generator of the field C_h, we see that the field determined by K and Z, whose degree is at most $l^{2h-1}(l-1)$, includes the field $k(\mathsf{Z}, C_h)$ of degree $l^{2h-1}(l-1)$. So these two fields must be identical and the number $\kappa = K^{l^h}$ has the property described in Lemma 15.

We make a further remark. The field determined by Z and $\sqrt[l^h]{\kappa}$ is easily seen to be a cyclic extension of $k(\mathsf{Z})$ of relative degree l^h and hence has a unique subfield including $k(\mathsf{Z})$ which is a cyclic extension of $k(\mathsf{Z})$ of relative degree l. If C_1 is the subfield of C_h of degree l then the compositum of $k(\mathsf{Z})$ and C_1 must coincide with the field determined by Z and $\sqrt[l]{\kappa}$.

§102. Concerning Certain Prime Divisors of the Discriminant of a Cyclic Field of Degree l^h

Lemma 16. *Let C_h be a cyclic field of degree l^h where l is any prime number (even or odd) and let C_1 be the subfield of C_h of degree l. Then any prime divisor p of the discriminant of C_1 other than l satisfies the congruence $p \equiv 1 \pmod{l^h}$.*

Proof. We consider first the case where l is an odd prime number and $h = 1$. Suppose, by way of contradiction, that there exists a rational prime factor p of the discriminant of C_1 which is not congruent to 1 modulo l. Let $\zeta = e^{2\pi i/l}$; let r be a primitive root modulo l and let s be the automorphism $(\zeta : \zeta^r)$ in the group of the field $k(\zeta)$. If $\mathfrak{p}$ is a prime ideal of $k(\zeta)$ dividing p then, since $p \not\equiv 1 \pmod{l}$, it follows from Theorem 119 that the degree f of $\mathfrak{p}$ is greater than 1. Hence, according to Theorem 129, the decomposition field of $\mathfrak{p}$ has degree $e < l-1$; the remaining prime ideal factors of p are then

$$\mathfrak{p}' = s\mathfrak{p}, \ldots, \mathfrak{p}^{(e-1)} = s^{e-1}\mathfrak{p},$$

while $s^e\mathfrak{p} = \mathfrak{p}$, i.e.

$$\mathfrak{p}^{s^e-1} = 1. \tag{23.1}$$

Similarly for the prime ideals $\mathfrak{p}'$, $\mathfrak{p}''$, ... conjugate to $\mathfrak{p}$ we have the corresponding equations

$$(\mathfrak{p}')^{s^e-1} = 1, \ (\mathfrak{p}'')^{s^e-1} = 1, \ldots \tag{23.2}$$

According to Lemma 15 there is an integer κ in $k(\zeta)$ such that the two numbers ζ and $\sqrt[l]{\kappa}$ generate the compositum $k(\zeta, C_1)$ of $k(\zeta)$ and C_1 and furthermore κ^{s-r} is equal to the l-th power of a number in $k(\zeta)$. Since $s^e - 1$

and $s - r$ are polynomials in s which have no common factor modulo l there are three integer polynomials $\varphi(s)$, $\psi(s)$ and $\chi(s)$ in the variable s such that

$$1 = (s^e - 1)\varphi(s) + (s - r)\psi(s) + l\chi(s).$$

From this it follows that

$$\kappa = \kappa^{(s^e-1)\varphi(s)+(s-r)\psi(s)+l\chi(s)} = \kappa^{(s^e-1)\varphi(s)}\alpha^l$$

where α is a number in $k(\zeta)$. According to the equations (23.1) and (23.2) for the prime ideals $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$, ... which we established above, κ^{s^e-1} can be written as an integer or fraction for which neither numerator or denominator has any of $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$, ... as prime factor and hence are prime to p; the same holds for $\kappa^{(s^e-1)\varphi(s)}$. We write $\kappa^{(s^e-1)\varphi(s)} = \rho/a^l$ where ρ is an integer of $k(\zeta)$ prime to p and a is a rational integer. The field $k(\zeta, C_1)$ can then be generated by ζ and $\sqrt[l]{\rho}$. The relative discriminant of the number $\sqrt[l]{\rho}$ with respect to $k(\zeta)$ is $\pm l^l \rho^{l-1}$ and since ρ is prime to p it follows that the relative discriminant of $k(\zeta, C_1)$ with respect to $k(\zeta)$ is prime to p. Since the discriminant of $k(\zeta)$ is also prime to p it follows from Theorem 39 that the discriminant of $k(\zeta, C_1)$ and hence also, by Theorem 85, the discriminant of C_1 are not divisible by p, which contradicts our hypothesis that p is a factor of this discriminant.

In a similar way we establish the result of Lemma 16 for odd primes l in the case where the exponent h is greater than 1. We let $\mathsf{Z} = e^{2\pi i/l^h}$, take r to be a primitive root modulo l^h and let s be the automorphism $(\mathsf{Z} : \mathsf{Z}^r)$ of $k(\mathsf{Z})$. Let p be a prime factor of the discriminant of C_1 distinct from l; let $\mathfrak{p}$ be a prime ideal factor of p in $k(\mathsf{Z})$. If we suppose that $p \equiv 1 \pmod{l}$ but $p \not\equiv 1 \pmod{l^h}$ then the prime ideal $\mathfrak{p}$ lies in the subfield $k(\mathsf{Z}^l)$ of $k(\mathsf{Z})$, i.e. we have $\mathfrak{p}^{s^{l^{h-2}(l-1)}-1} = 1$ and similarly for the conjugate prime ideals $\mathfrak{p}'$, $\mathfrak{p}''$, ... we have the equations

$$(\mathfrak{p}')^{s^{l^{h-2}(l-1)}-1} = 1, (\mathfrak{p}'')^{s^{l^{h-2}(l-1)}-1} = 1, \ldots$$

Since r is a primitive root modulo l^h we have $r^{l^{h-2}(l-1)} \not\equiv 1 \pmod{l^h}$ and hence we can obtain three integer polynomials $\varphi(s)$, $\psi(s)$, $\chi(s)$ in s such that

$$l^{h-1} = (s^{l^{h-2}(l-1)} - 1)\varphi(s) + (s - r)\psi(s) + l^h\chi(s).$$

From this it follows, if κ is a number chosen as in Lemma 15, that

$$\kappa^{l^{h-1}} = \kappa^{(s^{l^{h-2}(l-1)}-1)\varphi(s)}\alpha^{l^h},$$

where α is a number in $k(\mathsf{Z})$. According to the properties of the prime ideals $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$, ... established above, $\kappa^{s^{l^{h+1}(l-1)}-1}$, and hence also $\kappa^{(s^{l^{h-2}(l-1)}-1)\varphi(s)}$ are numbers whose numerators and denominators are prime to p. We can thus express the second of these numbers in the form ρ/a^{l^h} where ρ is an integer in $k(\mathsf{Z})$ prime to p and a is a rational integer. Then $\sqrt[l]{\kappa} = \frac{\alpha}{a}\sqrt[l^h]{\rho}$,

whence $\rho = \sigma^{l^{h-1}}$ where σ is a number in $k(\mathsf{Z})$. We remarked at the end of Sect. 101 that the field generated by Z and $\sqrt[l]{\kappa}$ is identical with the compositum of $k(\mathsf{Z})$ and C_1. Since the relative discriminant of the number $\sqrt[l]{\sigma}$ with respect to $k(\mathsf{Z})$ has the value $\pm l^l \sigma^{l-1}$ and so is prime to p, it follows that the relative discriminant of the field $k(\mathsf{Z}, C_1)$ with respect to $k(\mathsf{Z})$ is prime to p. The discriminant of $k(\mathsf{Z})$ is not divisible by p. Hence the same holds for the discriminant of $k(\mathsf{Z}, C_1)$ and hence also for the discriminant of C_1. This last statement, however, contradicts our hypothesis that p is a factor of this discriminant.

To establish the validity of Lemma 16 for $l = 2$ we start with the case $h = 2$ and apply Lemma 15 to the cyclic field C_2 of degree 4. We set $\mathsf{Z} = e^{\pi i/2} = i$ and consider the automorphism $s' = (i : -i)$ in the group of $k(\mathsf{Z})$. Let C_1 be the quadratic subfield of C_2. Suppose there were an odd prime divisor p of the discriminant of C_1 such that $p \not\equiv 1 \pmod 4$. As a result of this property p does not split in $k(i)$. If now the number κ given by Lemma 15 is divisible by p we introduce the number $\rho = \kappa^{s'-1}$. Since, according to Lemma 15, we also have $\kappa^{s'+1} = \alpha^4$ where α is a number in $k(i)$, it follows that $\kappa^2 = \rho^{-1}\alpha^4$, i.e. $\sqrt{\kappa} = \alpha\sqrt[4]{\rho^{-1}}$; consequently ρ is the square of a number in $k(i)$. We can write $\rho = \tau^2/a^4$ where τ is an integer of $k(i)$ prime to p and a is a rational integer. Since the field $k(i, C_1)$ coincides with the field $k(i, \sqrt{\tau})$ and the relative discriminant of $\sqrt{\tau}$ with respect to $k(i)$ is prime to p, we have that the relative discriminant of $k(i, C_1)$ with respect to $k(i)$ is prime to p; from this it follows that the discriminant of C_1 is not divisible by p and this contradicts our hypothesis that p divides the discriminant of C_1.

In the case where $l = 2$ and the exponent $h > 2$ we set $\mathsf{Z} = e^{\pi i/2^{h-1}}$. We suppose that there were a prime factor p of the discriminant of C_1 such that $p \equiv 1 \pmod 4$ but $p \not\equiv 1 \pmod{2^h}$. Let $\mathfrak{p}$ be a prime ideal of $k(i)$ dividing p; then $\mathfrak{p}$ is invariant under an automorphism $s_*^{2^{h-3}}$ where s_* is taken to be either $(\mathsf{Z} : \mathsf{Z}^5)$ or $(\mathsf{Z} : \mathsf{Z}^{-5})$; consequently $\mathfrak{p}^{s_*^{2^{h-3}}-1} = 1$. Since $(\pm 5)^{2^{h-3}} \not\equiv 1 \pmod{2^h}$ then, in the same way as before, we have an equation of the form

$$2^{h-1} = (s_*^{2^{h-3}} - 1)\varphi(s_*) + (s_* \mp 5)\psi(s_*) + 2^h \chi(s_*).$$

From this, as in the earlier case where l is odd, we deduce a contradiction to the hypothesis that p divides the discriminant of C_1.

This completes the proof of Lemma 16.

The following result is easily deduced from Lemma 16.

Lemma 17. *Let C_h be a cyclic field of degree l^h where l is a prime number (even or odd); let C_1 be the subfield of C_h of degree l; let p be a prime divisor of the discriminant of C_1 other than l. Then there exists an abelian field $C'_{h'}$ of some degree $l^{h'}$ not exceeding l^h with the following properties:*

(1) *The compositum of $C'_{h'}$ with some cyclotomic field P_h includes C_h as a subfield;*

(2) *The discriminant of $C'_{h'}$ is divisible only by those rational prime numbers which divide the discriminant of C_h with the exception of p.*

Proof. According to Lemma 16 the rational prime number p has the property that $p \equiv 1 \pmod{l^h}$. As in Sect. 100 we construct a (cyclic) cyclotomic field P_h of degree l^h whose discriminant is a power of p; consider the compositum $k(C_h, P_h)$ of C_h and P_h and let the degree of this compositum be $l^{h+h'}$. In P_h we have $p = \mathfrak{p}^{l^h}$ where $\mathfrak{p}$ is a prime ideal of P_h. Let $\mathfrak{P}$ be a prime ideal of $k(C_h, P_h)$ which divides $\mathfrak{p}$. Since this prime ideal $\mathfrak{P}$ does not divide the degree $l^{h+h'}$ of $k(C_h, P_h)$ it follows that $k(C_h, P_h)$ is the ramification field of $\mathfrak{P}$ and hence, according to Theorem 81, is a cyclic extension of degree at least l^h of the inertia field of $\mathfrak{P}$, which we denote by $C'_{h'}$. Since there can be no cyclic fields of degree greater than l^h in $k(C_h, P_h)$ it follows that $k(C_h, P_h)$ has degree exactly l^h over $C'_{h'}$; hence the field $C'_{h'}$ has degree $l^{h'}$. According to Theorem 76 the different of the inertia field $C'_{h'}$ is not divisible by $\mathfrak{P}$ and so, as a result of Theorem 68, the discriminant of $C'_{h'}$ is not divisible by p. On the other hand, we see from Theorem 39 that this discriminant is divisible only by those prime numbers which are factors of the discriminant of C_h. Finally it follows from Theorem 87 that the compositum of $C'_{h'}$ and P_h coincides with $k(C_h, P_h)$. Thus the field $C'_{h'}$ has all the properties described in Lemma 17.

§103. The Cyclic Field of Degree u Whose Discriminant is Divisible Only by u and Cyclic Fields of Degree u^h and 2^h Including U_1 and II_1 Respectively as Subfields

Lemma 18. *If the discriminant of a cyclic field of odd prime degree u has no prime factors other than u then $C_1 = U_1$.*

Proof. We set $\zeta = e^{2\pi i/u}$ and $s = (\zeta : \zeta^r)$ where r is a primitive root modulo u. We write $\lambda = 1 - \zeta$, so that $\mathfrak{l} = (\lambda)$ is a prime ideal in $k(\zeta)$ and u (considered as an ideal) is $\mathfrak{l}^{u-1}$; in addition we have the congruence

$$s\lambda = 1 - \zeta^r \equiv r\lambda \pmod{\mathfrak{l}^2}.$$

We consider now the number κ described in Lemma 15. Since the prime ideal $\mathfrak{l}$ is of degree 1 and $s\mathfrak{l} = \mathfrak{l}$ it follows from Theorem 24 that if we set $\rho = \kappa^{(s-1)(u-1)}$ then $\rho \equiv 1 \pmod{\mathfrak{l}}$, where we understand a congruence between fractions to hold if it is transformed into a valid ordinary congruence on multiplication by an integer relatively prime to the modulus. Since $r-1$ is prime to u the compositum of C_1 and $k(\zeta)$ is generated also by ζ and $\sqrt[u]{\rho}$. If we have $\rho \equiv 1 + a\lambda \pmod{\mathfrak{l}^2}$ where a is a rational integer then $\sigma = \rho\zeta^a \equiv 1 \pmod{\mathfrak{l}^2}$.

We now prove that $\sigma \equiv 1 \pmod{\mathfrak{l}^u}$. To this end we suppose that $\sigma \equiv 1 + a\lambda^e \pmod{\mathfrak{l}^{e+1}}$ where the exponent $e < u$ and a is a rational integer not divisible by u.

We recall that, according to Lemma 15, κ^{s-r} and hence also σ^{s-r} is the u-th power of a number in $k(\zeta)$; we set $\sigma^{s-r} = \beta^u$ where β is in $k(\zeta)$. This equation leads to the congruence $1 + a(r\lambda)^e - ar\lambda^e \equiv \beta^u \pmod{\mathfrak{l}^{e+1}}$. From this we deduce first that $\beta \equiv 1 \pmod{\mathfrak{l}}$ and hence $\beta^u \equiv 1 \pmod{\mathfrak{l}^u}$. Finally we have $ar^e \equiv ar \pmod{\mathfrak{l}}$ which is impossible since r is a primitive root modulo u and $e > 1$. These considerations establish the congruence $\sigma \equiv 1 \pmod{\mathfrak{l}^u}$.

We now set $\sigma = \tau/a^{u(u-1)}$ where τ is an integer in $k(\zeta)$ and a is a rational integer; then $\tau \equiv 1 \pmod{\mathfrak{l}^u}$. Let us suppose that C_1 is not identical with the field U_1. Then the compositum of $k(\zeta)$, U_1 and C_1 is the field $k(\sqrt[u]{\zeta}, \sqrt[u]{\tau})$ of degree $u^2(u-1)$ generated by $\sqrt[u]{\zeta}$ and $\sqrt[u]{\tau}$. Let $\xi = (1 - \sqrt[u]{\tau})/\lambda$; then the equation

$$\frac{(\xi\lambda - 1)^u + \tau}{\lambda^u} = 0$$

shows that ξ is an integer of the field $k(\sqrt[u]{\zeta}, \sqrt[u]{\tau})$ and its relative discriminant with respect to $k(\sqrt[u]{\zeta})$ is $\varepsilon\tau^{u-1}$ where ε is a unit. Since τ is prime to u it follows that the relative discriminant of the field $k(\sqrt[u]{\zeta}, \sqrt[u]{\tau})$ with respect to $k(\sqrt[u]{\zeta})$ is also prime to u. Let $\mathfrak{L}^*$ be a prime ideal of $k(\sqrt[u]{\zeta}, \sqrt[u]{\tau})$ dividing $\mathfrak{l}$. Then, taking account of Theorem 93, we see that the inertia field T of $\mathfrak{L}^*$ in $k(\sqrt[u]{\zeta}, \sqrt[u]{\tau})$ has degree u. The discriminant of this inertia field T is prime to u and according to Theorem 85 it must therefore be either $+1$ or -1. But there is no cyclic field of degree u with discriminant ± 1: this follows either directly from Theorem 44 or by means of Theorem 94 if we take the field k there to be the rational number field and recall that in this field all ideals are principal.

This completes the proof of Lemma 18.

Lemma 19. *Let C_h be a cyclic field of degree l^h where l is either an odd prime number u or equal to 2. If C_h includes U_1 or II_1 in these two cases respectively then C_h is a subfield of the compositum of U_h or II_h respectively with a cyclic field $C'_{h'}$ of degree $l^{h'}$ less than l^h.*

Proof. Suppose $C_h \neq U_h$ or II_h respectively. Let L_{h^*} be the largest subfield included in both C_h and U_h or C_h and II_h respectively. Let the degree of L_{h^*} be l^{h^*} where h^* is a positive integer less than h. Let t be an automorphism of the field C_h which generates the group of C_h; let z be an automorphism which generates the group of U_h or II_h respectively. Set $t^* = t^{l^{h^*}}$ and $z^* = z^{l^{h^*}}$; then t^* and z^* respectively generate the subgroups of order l^{h-h^*} to which L_{h^*} belongs as subfield of C_h and of U_h or II_h. The compositum K of C_h and U_h or II_h has relative degree l^{2h-2h^*} over L_{h^*} and so finally K has degree l^{2h-h^*}.

In order to determine the group G of the field K let ϑ be a generator of C_h and γ a generator of U_h or II_h; let x and y be indeterminates. Then $\Theta = x\vartheta + y\gamma$ satisfies an equation of degree l^{2h-h^*} whose coefficients are integer polynomials in x and y and which is irreducible over the field generated by x and y. The roots of this equation have the form

$$\Theta_{mn} = xt^m\vartheta + yz^n\gamma,$$

where m, n are certain rational integers. Since by a well-known theorem both ϑ and γ can be expressed as rational functions of Θ in which the coefficients are integer polynomials in x and y it follows that the expressions Θ_{mn} can be represented in the same way; we set

$$\Theta_{mn} = xt^m\vartheta + yz^n\gamma = \Phi_{mn}(\Theta)$$

where Φ_{mn} is a rational function of Θ whose coefficients are integer polynomials in x and y. Let A be any number in K or more generally a rational function of x and y with coefficients in K; then A can be expressed as a rational function $F(\Theta)$ of Θ whose coefficients are integer polynomials in x and y. The quantities conjugate to A can be expressed in the form

$$S_{mn}\mathsf{A} = F(\Phi_{mn}(\Theta))$$

and the corresponding l^{2h-h^*} automorphisms S_{mn} form the group G of the field K. Since

$$S_{mn}\Theta = xS_{mn}\vartheta + yS_{mn}\gamma = xt^m\vartheta + yz^z\gamma$$

we have

$$S_{mn}\vartheta = t^m\vartheta, \quad S_{mn}\gamma = z^n\gamma,$$

from which it follows easily that

$$S_{mn}S_{m'n'} = S_{m+m',n+n'} \tag{23.3}$$

where $S_{mn} = S_{m^*n^*}$ when $m \equiv m^*$ and $n \equiv n^*$ (mod l^h). From (23.3) we deduce that the automorphisms in the group G commute, i.e. K is an abelian field.

Let r be a primitive root modulo l^h. Since in particular $z^r\gamma$ is a conjugate of γ there must be an automorphism in G for which the second index n is congruent to r modulo l^h. We denote such an automorphism S_{mr} by s. The order of the cyclic group generated by s is l^h. Furthermore it can be easily established that all the automorphisms in the group G for which the second index is congruent to 0 modulo l^h form a cyclic subgroup of order l^{h-h^*}. Let $s^* = S_{m^*0}$ be an automorphism which generates this cyclic subgroup. The group G is then obviously formed by combining all l^h powers of s and all l^{h-h^*} powers of s^*. The subfield of K belonging to the cyclic subgroup generated by s^* is clearly the cyclic subfield U_h or II_h. The subfield belonging to the cyclic subgroup generated by s is a cyclic subfield $C'_{h'}$ of degree l^{h-h^*}.

The field $C'_{h'}$ has no subfield in common with U_h or II_h other than the field of rational numbers; thus K is the compositum of the cyclic fields $C'_{h'}$ and U_h or $C'_{h'}$ and II_h.

This completes the proof of Lemma 19.

§104. Proof of the Fundamental Theorem on Abelian Fields

We proceed to prove the fundamental Theorem 131 as follows. First of all, it was established in Sect. 48 that every abelian field is composed of cyclic fields whose degrees are either prime numbers or powers of a prime; hence we have only to show that every cyclic field C_h of degree l^h, where l is a prime number, is a cyclotomic field.

To prove this we proceed inductively; so we suppose that the conclusion of Theorem 131 holds for all abelian fields with degree any power of l less than l^h.

Consider now the subfield C_1 of degree l included in C_h and suppose that the discriminant of C_1 is divisible by a rational prime number p distinct from l; by Theorem 39 it follows that the discriminant of C_h is also divisible by p. Then, according to Lemma 17, there is an abelian field $C'_{h'}$ of degree $l^{h'}$ not exceeding l^h such that C_h is a subfield of the compositum of $C'_{h'}$ and a cyclotomic field P_h. If $C'_{h'}$ is a cyclic field of degree less than l^h or the compositum of several such cyclic fields then, according to our inductive hypothesis, $C'_{h'}$ is a cyclotomic field and hence so also is C_h. So we have only to consider the case where $h' = h$ and $C'_{h'} = C'_h$ is a cyclic field of degree l^h. Referring again to Lemma 17 we see that the discriminant of C'_h is divisible only by those rational primes which divide the discriminant of C_h with the exception of p; so the discriminant of C'_h has at least one prime factor fewer than the discriminant of C_h.

We denote the subfield of C'_h of degree l by C'_1. If the discriminant of C'_1 has a rational prime factor p' distinct from l then we can apply to C'_h the same procedure as we have just used for the original field C_h and so either conclude that C'_h is a cyclotomic field or else find a cyclic field C''_h of degree l^h whose discriminant has at least one prime factor (namely p') fewer than the discriminant of C'_h. After repeating this procedure a certain number of times, say m, we either obtain a field $C^{(m)}_{h^{(m)}}$ which is cyclotomic in consequence of the inductive hypothesis or else a cyclic field $C^{(m)}_h$ of degree l^h such that the discriminant of the subfield $C^{(m)}_1$ of degree l in $C^{(m)}_h$ has either no rational prime factor or only the factor l. Since, as we remarked on p.184, there is no cyclic field of degree l with discriminant ± 1, only the latter case can arise.

We now distinguish two cases, according as l is an odd prime number or $l = 2$.

In the first case $C^{(m)}_1$ coincides with U_1 by Lemma 18.

In the second case, where $l = 2$, if $h = 1$ then the field $C_1^{(m)}$ is either $k(i)$ or $k(\sqrt{2}) = II_1$ and hence obviously a cyclotomic field. For $h > 1$ the field $C_1^{(m)}$ always turns out to be $k(\sqrt{2}) = II_1$. For if $C_h^{(m)}$ is a real field then $C_1^{(m)}$ is also real and our assertion follows, while if $C_h^{(m)}$ is an imaginary field then the real numbers in it form a subfield of degree 2^{h-1} and since $C_1^{(m)}$ must be included in this subfield it is also real and so coincides with II_1.

In both the cases just considered except when $l = 2$ and $h = 1$ we have $C_1^{(m)} = U_1$ or II_1. By Lemma 19 it follows that $C_h^{(m)}$ is a subfield of the compositum of U_h or II_h and a cyclic field $C_{\bar{h}}$ of degree $l^{\bar{h}}$ less than l^h. According to the inductive hypothesis the conclusion of Theorem 131 holds for such cyclic fields $C_{\bar{h}}$; so it follows that $C_h^{(m)}$ is a cyclotomic field.

This completes the proof of the fundamental Theorem 131 and at the same time it is clear how we can determine all abelian fields with given group and given discriminant.

24. The Root Numbers of the Cyclotomic Field of the l-th Roots of Unity

§105. Definition and Existence of Normal Bases

A basis of an abelian field K of degree M is called a *normal basis* if it consists of an integer N and its conjugates $\mathsf{N}', \ldots, \mathsf{N}^{(M-1)}$. We have the following lemma.

Lemma 20. *If an abelian field K has a normal basis then so also does every subfield k of K.*

Proof. Let M be the degree of K and let $t_1, \ldots, t_M$ be the automorphisms in the group of the abelian field K; let N be an integer of K which, together with its conjugates, forms a normal basis of K. Let $t_1, \ldots, t_r$ be the automorphisms in the subgroup belonging to the subfield k of K. Then, among $t_1, \ldots, t_M$ we can find $m = M/r$ automorphisms $t_1', \ldots, t_m'$ such that (apart from order) the automorphisms $t_1, \ldots, t_M$ can be represented as

$$t_1't_1, \ldots, t_1't_r, t_2't_1, \ldots, t_2't_r, \ldots, t_m't_1, \ldots, t_m't_r.$$

Let α be an integer in k. Then, since α is also an integer in K, we have an equation

$$\alpha = a_{11}t_1't_1\mathsf{N} + \cdots + a_{1r}t_1't_r\mathsf{N} + \cdots + a_{m1}t_m't_1\mathsf{N} + \cdots + a_{mr}t_m't_r\mathsf{N}$$

where $a_{11}, \ldots, a_{1r}, \ldots, a_{m1}, \ldots, a_{mr}$ are rational integers. We recall that α is invariant under the action of the automorphisms $t_1, \ldots, t_r$ and that there is no linear relation between the $M = mr$ numbers $t_1't_1\mathsf{N}, \ldots, t_1't_r\mathsf{N}, \ldots, t_m't_1\mathsf{N}, \ldots, t_m't_r\mathsf{N}$ with rational integer coefficients not all zero. It follows that

$$a_{11} = a_{12} = \cdots = a_{1r}, \ \ldots, \ a_{m1} = a_{m2} = \cdots = a_{mr}.$$

Thus, if we set

$$\nu = t_1\mathsf{N} + t_2\mathsf{N} + \cdots + t_r\mathsf{N},$$

then the m numbers $t_1'\nu, t_2'\nu, \ldots, t_m'\nu$ form a normal basis for k.

Theorem 132. *Every abelian field K of degree M whose discriminant D is prime to M has a normal basis.*

Proof. Let $p, p', \ldots$ be the distinct rational prime divisors of D. Since none of these prime numbers divides M we deduce from the proof of Theorem 131 that the abelian field K is included as a subfield in the cyclotomic field generated by the numbers $\zeta = e^{2\pi i/p}$, $\zeta' = e^{2\pi i/p'}, \ldots$, i.e. the field determined by the root of unity $Z = e^{2\pi i/pp'\cdots}$. According to Theorem 118 the numbers $1, \zeta, \ldots, \zeta^{p-2}$, and hence also the numbers $\zeta, \zeta^2, \ldots, \zeta^{p-1}$ form a basis for the field $k(\zeta)$; this latter basis is a normal basis. We have similar results for $k(\zeta'), \ldots$.

Now we consider the set of $(p-1)(p'-1)\cdots$ numbers $\zeta^h(\zeta')^{h'}\ldots$ where the exponents $h, h', \ldots$ run (independently of one another) through the sets $1, 2, \ldots, p-1$; $1, 2, \ldots, p'-1, \ldots$. According to Theorem 88 this set of $\Phi(pp'\cdots)$ numbers forms a basis for the field $k(Z)$ and it is obviously a normal basis. Lemma 20 then shows that the abelian field K also has a normal basis.

This completes the proof of Theorem 132.

§106. Abelian Fields of Prime Degree l and Discriminant p^{l-1}. Root Numbers of This Field

The simplest and most important abelian fields after the quadratic fields are those whose degree is an odd prime number l and whose discriminant d is divisible by a single prime number p distinct from l. Let k be such a field. By Lemma 16 the prime p must be such that $p \equiv 1 \pmod{l}$. In k the prime p must be the l-th power of a prime ideal of degree 1. According to the remarks after Theorem 79 and the fact that k is in this case a real field (and so d is positive) we have the result that $d = p^{l-1}$.

Let $1, t, t^2, \ldots, t^{l-1}$ be the automorphisms in the group of k; let $\nu, t\nu, t^2\nu, \ldots, t^{l-1}\nu$ be a normal basis for k (see Theorem 132). The number ν is then a generator of the field k. If we set $\zeta = e^{2\pi i/l}$ the expression

$$\Omega = \nu + \zeta \cdot t\nu + \zeta^2 \cdot t^2\nu + \cdots + \zeta^{l-1} \cdot t^{l-1}\nu$$

is called a *root number* of the field $k = k(\nu)$.

Each such root number is clearly an integer of the compositum $k(\nu, \zeta)$ of $k(\nu)$ and $k(\zeta)$. Study of the normal bases and root numbers we have introduced leads us to important information about the prime ideals of $k(\zeta)$ dividing p. The development of this chapter needs only slight modification when we take l to be 2 instead of an odd prime number.

§107. Characteristic Properties of Root Numbers

Theorem 133. *Let k be an abelian field of degree l and discriminant $d = p^{l-1}$, where l and p are distinct odd prime numbers. Let $\nu, t\nu, \ldots, t^{l-1}\nu$ form a normal basis of the field k. Set $\zeta = e^{2\pi i/l}$, $\mathfrak{l} = (1-\zeta)$ and $s = (\zeta : \zeta^r)$,*

where r is a primitive root modulo l. Then the root number Ω of the field $k = k(\nu)$ derived from the normal basis has the following properties:

(1) *The l-th power $\omega = \Omega^l$ of the root number belongs to the cyclotomic field $k(\zeta)$ and ω^{s-r} is the l-th power of a number in $k(\zeta)$.*

(2) *The (equivalent) congruences*

$$\Omega \equiv \pm 1 \pmod{\mathfrak{l}} \quad \text{and} \quad \omega \equiv \pm 1 \pmod{\mathfrak{l}^l}$$

are satisfied.

(3) *The norm of the number ω in $k(\zeta)$ is $n(\omega) = p^{\frac{1}{2}l(l-1)}$.*

Proof. The numbers Ω^l and Ω^{s-r} in $k(\zeta, \nu)$ are unaltered when ν is replaced by $t\nu$; hence they lie in $k(\zeta)$. So we have established the first assertion of the theorem.

Since ν, $t\nu$, $\ldots$, $t^{l-1}\nu$ form a basis of $k(\nu)$ there are rational integers $a_0, a_1, \ldots, a_{l-1}$ such that

$$1 = a_0\nu + a_1 t\nu + \cdots + a_{l-1}t^{l-1}\nu.$$

Applying the automorphism t to this relation we see that $a_0 = a_1 = \cdots = a_{l-1}$ and since the coefficients $a_0, a_1, \ldots, a_{l-1}$ can have no common factor other than ± 1 they must be equal to ± 1. Thus we have

$$\nu + t\nu + \cdots + t^{l-1}\nu = \pm 1.$$

It follows that

$$\begin{aligned} \Omega &= \nu + \zeta \cdot t\nu + \zeta^2 \cdot t^2\nu + \cdots + \zeta^{l-1} \cdot t^{l-1}\nu \\ &\equiv \nu + t\nu + \cdots + t^{l-1}\nu \equiv \pm 1 \pmod{\mathfrak{l}}. \end{aligned}$$

From the fact that $\omega \mp 1 = (\Omega \mp 1)(\zeta\Omega \mp 1)\cdots(\zeta^{l-1}\Omega \mp 1)$ we obtain the second property of the number ω.

Finally, by an appropriate application of the multiplication theorem for determinants, we have

$$\begin{vmatrix} \nu & t\nu & \ldots & t^{l-1}\nu \\ t^{l-1}\nu & \nu & \ldots & t^{l-2}\nu \\ & & \ldots\ldots & \\ t\nu & t^2\nu & \ldots & \nu \end{vmatrix} = (\nu + t\nu + \cdots + t^{l-1}\nu)n(\Omega) = \pm n(\Omega),$$

where

$$n(\Omega) = (\nu + \zeta \cdot t\nu + \cdots + \zeta^{l-1} \cdot t^{l-1}\nu) \cdots (\nu + \zeta^{l-1} \cdot t\nu + \cdots + \zeta^{(l-1)^2} \cdot t^{l-1}\nu)$$

is the relative norm of Ω with respect to the field $k(\nu)$. The square of the determinant on the left hand side is equal to the discriminant of the field $k(\nu)$, i.e. to p^{l-1}, and hence we have

$$n(\omega) = (n(\Omega))^l = p^{\frac{1}{2}l(l-1)}.$$

This completes the proof of Theorem 133.

Conversely, the three properties of a root number Ω proved in Theorem 133 actually give a complete characterization of such root numbers. We have in fact the following result.

Theorem 134. *Let l be an odd prime, $\zeta = e^{2\pi i/l}$ and p a prime number congruent to 1 modulo l. Let ω be a number in the cyclotomic field $k(\zeta)$ which is not the l-th power of a number in $k(\zeta)$ but which satisfies the three properties described in Theorem 133. Then $\Omega = \sqrt[l]{\omega}$ is a root number of the abelian field of degree l with discriminant p^{l-1}.*

Proof. The number $\Omega = \sqrt[l]{\omega}$ generates a Galois extension of $k(\zeta)$ of relative degree l. Let t be the automorphism in the group of this extension for which $t\Omega = \zeta^{-1}\Omega$. As a consequence of the first property of ω, which asserts that $s\omega = \omega^r\alpha^l$ where α is a number in $k(\zeta)$, we deduce that the field generated by ζ and Ω is a Galois number field of degree $l(l-1)$. The number α satisfies the condition

$$\omega^{1-r^{l-1}} = \alpha^{l\cdot(s^{l-1}-r^{l-1})/(s-r)};$$

We fix it uniquely by the additional requirement that

$$\omega^{(1-r^{l-1})/l} = \alpha^{(s^{l-1}-r^{l-1})/(s-r)}.$$

We now understand by t and s those automorphisms in the group of the Galois number field $k(\zeta,\Omega)$ which in addition to the relations already laid down for t and s have the further properties that $t\zeta = \zeta$ and $s\Omega = \Omega^r\alpha$. These two automorphisms commute with one another since

$$st\Omega = \zeta^{-r}\Omega^r\alpha = ts\Omega;$$

Thus $k(\zeta,\Omega)$ is an abelian field. The subgroup of the group of $k(\zeta,\Omega)$ consisting of the powers of the automorphism s has order $l-1$. So the subfield k of $k(\zeta,\Omega)$ belonging to this subgroup has degree l; it is again an abelian field.

We prove first that the discriminant of the field k is prime to l. Since Ω is congruent to ± 1 modulo $\mathfrak{l} = (1-\zeta)$ the quotient $\dfrac{\Omega \mp 1}{1-\zeta}$ is an integer. Since $t\Omega = \zeta^{-1}\Omega$ the relative different of this integer with respect to $k(\zeta)$ has the form $\varepsilon\Omega^{l-1}$, where ε is a unit. Hence the relative different of $k(\zeta,\Omega)$ with respect to $k(\zeta)$ is prime to l. If $\mathfrak{L}$ is a prime ideal of $k(\zeta,\Omega)$ which divides $\mathfrak{l}$ it follows from Theorem 93 that it cannot divide $\mathfrak{l}$ to any power higher than the first; hence we have $l = \mathfrak{L}^{l-1}\mathfrak{M}$ where $\mathfrak{M}$ is not divisible by $\mathfrak{L}$. Thus it follows from Sect. 39 and Sect. 40 that the inertia field of the prime ideal $\mathfrak{L}$ must have degree l; hence this inertia field must be the field k. According to Theorem 76 the different of k is not divisible by $\mathfrak{L}$ and hence, by Theorem 68, the discriminant of k is not divisible by l.

We set
$$\nu = \frac{\pm 1 + \Omega + s\Omega + s^2\Omega + \cdots + s^{l-1}\Omega}{l} \tag{24.1}$$
where the sign is the same as in the congruences $\Omega \equiv \pm 1$, $s\Omega \equiv \pm 1$, ... (mod $\mathfrak{l}$); then the numerator of the fractional expression in (24.1) is congruent to 0 modulo $\mathfrak{l}$. This numerator lies in the field k. If l is a prime ideal of k this numerator must also be divisible by l and hence ν is an integer. Otherwise, since the discriminant of k is not divisible by l, we would have a factorisation $l = \mathfrak{l}_1 \dots \mathfrak{l}_l$ in k where $\mathfrak{l}_1, \dots, \mathfrak{l}_l$ are distinct prime ideals. Then, as a consequence of Theorem 88, we have in $k(\zeta, \Omega)$ the factorisation
$$\mathfrak{l} = (1-\zeta) = (\mathfrak{l}, \mathfrak{l}_1)(\mathfrak{l}, \mathfrak{l}_2) \dots (\mathfrak{l}, \mathfrak{l}_l).$$
Since the numerator of the fraction on the right hand side of (24.1) is divisible by the ideal $(\mathfrak{l}, \mathfrak{l}_1)$ it is also, considered as an integer of k, divisible by $\mathfrak{l}_1$. Similarly this numerator is divisible by $\mathfrak{l}_2, \dots, \mathfrak{l}_l$ and hence by l; thus the number ν defined by (24.1) is an integer.

Using the equation $t\Omega = \zeta^{-1}\Omega$ we may derive from (24.1) the two equations
$$\nu + t\nu + t^2\nu + \cdots + t^{l-1}\nu = \pm 1 \tag{24.2}$$
$$\nu + \zeta \cdot t\nu + \zeta^2 \cdot t^2\nu + \cdots + \zeta^{l-1} \cdot t^{l-1}\nu = \Omega. \tag{24.3}$$
An application of the multiplication theorem for determinants like that in the proof of Theorem 133 gives
$$\mathsf{N} = \begin{vmatrix} \nu & t\nu & \dots & t^{l-1}\nu \\ t^{l-1}\nu & \nu & \dots & t^{l-2}\nu \\ & & \dots\dots & \\ t\nu & t^2\nu & \dots & \nu \end{vmatrix} = \pm\Omega \cdot s\Omega \cdot \dots \cdot s^{l-2}\Omega,$$
and from this, using the third property of ω in Theorem 133, we deduce the equation
$$\mathsf{N}^l = \pm p^{\frac{1}{2}l(l-1)}$$
and hence
$$\begin{vmatrix} \nu & t\nu & \dots & t^{l-1}\nu \\ t^{l-1}\nu & \nu & \dots & t^{l-2}\nu \\ & & \dots\dots & \\ t\nu & t^2\nu & \dots & \nu \end{vmatrix}^2 = p^{l-1}.$$

We now prove that the discriminant of k must be p^{l-1}. According to the last equation it must be a positive factor of p^{l-1}. Since, by Theorem 44 or Theorem 94, it cannot be 1 it must have p as a factor and indeed, according to the remarks on Theorem 79, to the $(l-1)$-st power. From the fact we have just proved it follows that $\nu, t\nu, \dots, t^{l-1}\nu$ form a basis of the field k; this is clearly a normal basis. According to (24.3) Ω is the root number of k arising from this normal basis.

§108. Factorisation of the l-th Power of a Root Number in the Field of the l-th Roots of Unity

Theorem 135. *Let l, p, ζ, r, s have the same meaning as before; let $k(\nu)$ be an abelian field of degree l with discriminant p^{l-1} and Ω a root number of $k(\nu)$. Then $\omega = \Omega^l$ splits in $k(\zeta)$ as the*

$$(r_0 + r_{-1}s + r_{-2}s^2 + \cdots + r_{-l+2}s^{l-2})th$$

power of $\mathfrak{p}$ where $\mathfrak{p}$ is a certain prime ideal of $k(\zeta)$ dividing p and in general r_{-i} is the least positive rational integer which is congruent modulo l to the $(-i)$-th power r^{-i} of the primitive root r (Kummer (6, 11)).

Proof. The prime number p splits in $k(\zeta)$ as the product of $l-1$ distinct prime ideal factors $\mathfrak{p}$, $s\mathfrak{p}$, ..., $s^{l-2}\mathfrak{p}$. We claim that the number ω must be divisible by each of these prime ideals. For, according to the proof of Theorem 134, the relative different of $k(\zeta, \Omega)$ with respect to $k(\zeta)$ is a factor of $\Omega^l = \omega$; if ω were prime to $\mathfrak{p}$ say, then this relative different would be prime to $\mathfrak{p}$. Hence, by Theorem 41, the different of $k(\zeta, \Omega)$ and so also, by Theorem 68, the discriminant of $k(\zeta, \Omega)$ would be prime to p, which is not possible since it has the discriminant of $k(\nu)$ as a factor. Since $n(\omega) = p^{\frac{1}{2}l(l-1)}$ it follows that $\mathfrak{p}$, $s\mathfrak{p}$, ..., $s^{l-2}\mathfrak{p}$ are the only prime ideals dividing ω. Let $\mathfrak{p}$ be one of these prime ideals which occurs in ω to the lowest possible power; then we have

$$\omega = \mathfrak{p}^{a_0 + a_1 s + \cdots + a_{l-2}s^{l-2}},$$

where a_0, a_1, ..., a_{l-2} are rational integers none of which is less than a_0. The formation of $n(\omega)$ shows us that

$$a_0 + a_1 + \cdots + a_{l-2} = \tfrac{1}{2}l(l-1).$$

Since a_0, a_1, ..., a_{l-2} are all positive it follows from this that these numbers cannot all be divisible by l. As a result of the first property established in Theorem 133 we have

$$\omega^{s-r} = \mathfrak{p}^{(s-r)(a_0 + a_1 s + \cdots + a_{l-2}s^{l-2})} = \alpha^l,$$

where α is a number in $k(\zeta)$. Since the prime ideals conjugate to $\mathfrak{p}$ are all distinct from $\mathfrak{p}$ and from each other it follows that when we multiply out the polynomial

$$(s-r)(a_0 + a_1 s + \cdots + a_{l-2}s^{l-2})$$

and set $s^{l-1} = 1$ all the coefficients must be divisible by l and so this polynomial must be congruent to $a_{l-2}(s^{l-1} - 1)$ modulo l. Thus we see that $a_{l-2} \not\equiv 0 \pmod{l}$ and if $a_{l-2} \equiv r^{m-l+2} \pmod{l}$, where m is one of the numbers 0, 1, ..., $l-2$ then for each index $i = 0, 1, \ldots, l-2$ we have the congruence

$$a_i \equiv r^{m-i} \pmod{l}.$$

In general we set $a_i = r_{m-i} + lb_i$ with $0 < r_{m-i} < l$ and b_i a rational integer; we always have $b_i \geq 0$. Since

$$r_m + r_{m-1} + \cdots + r_{m-l+2} = 1 + 2 + \cdots + (l-1) = \tfrac{1}{2}l(l-1)$$

it follows that $b_0 + b_1 + \cdots + b_{l-2} = 0$ and hence

$$b_0 = 0, b_1 = 0, \ldots, b_{l-2} = 0;$$

that is to say

$$a_i = r_{m-i} \quad \text{for } i = 0, 1, \ldots, l-2.$$

Among the numbers $r_0, r_1, \ldots, r_{l-2}$ it is clear that r_0 is the least; and since a_0 is the least among the coefficients $a_0, a_1, \ldots, a_{l-2}$ it follows that $a_0 = r_0 = 1$. Hence $m = 0$ and so, in general, $a_i = r_{-i}$.

This completes the proof of Theorem 135.

§109. An Equivalence for the Prime Ideals of Degree 1 in the Field of the l-th Roots of Unity

From the results we have developed so far we can deduce an important property of the prime ideals of the field of the l-th roots of unity which divide a prime number p congruent to 1 modulo l.

Theorem 136. *Let l be an odd prime number, $\zeta = e^{2\pi i/l}$, r a positive primitive root modulo l and $s = (\zeta : \zeta^r)$. If $\mathfrak{p}$ is any prime ideal of degree 1 in the cyclotomic field $k(\zeta)$ then*

$$\mathfrak{p}^{q_0 + q_{-1}s + q_{-2}s^2 + \cdots + q_{-l+2}s^{l-2}} \sim 1,$$

where the numbers q_{-i} are rational integers given by

$$q_{-i} = \frac{rr_{-i} - r_{-i+1}}{l} \qquad (i = 0, 1, \ldots, l-2).$$

(Here $r_0, r_{-1}, \ldots, r_{-l+2}$ have the same meaning as in Theorem 135 and in addition $r_1 = r_{-l+2}$.) (*Kummer* (6, 11)).

Proof. Let p and ω have the same meaning as in Theorem 133. Then, by Theorem 133, ω^{s-r} is the l-th power of a number α in $k(\zeta)$. If we introduce the representation of ω as a power of $\mathfrak{p}$ given in Theorem 135 then it follows that

$$\mathfrak{p}^{(s-r)(r_0 + r_{-1}s + \cdots + r_{-l+2}s^{l-2})} = \alpha^l$$

and when we deduce from this equation the factorisation of α the result of Theorem 136 follows.

Let C be any ideal class of the cyclotomic field $k(\zeta)$; if $\mathfrak{i}$ is an ideal in C and sC, $s^2C, \dots, s^{l-2}C$ are the ideal classes containing the ideals $s\mathfrak{i}$, $s^2\mathfrak{i}, \dots,$ $s^{l-2}\mathfrak{i}$ respectively, then it follows at once from Theorems 89 and 136 that

$$C^{q_0}(sC)^{q_{-1}}(s^2C)^{q_{-2}}\cdots(s^{l-2}C)^{q_{-l+2}} = 1.$$

§110. Construction of All Normal Bases and Root Numbers

Theorems 133, 134 and 135 make it possible for us to construct all the root numbers of the abelian field $k(\nu)$. We have the following result.

Theorem 137. *Let k be an abelian field of odd prime degree l with discriminant p^{l-1}; let t be a generator of the group of k. If Ω and Ω^* are distinct root numbers of k corresponding to t then $\Omega^* = \varepsilon\Omega$ where ε is a unit of the field $k(\zeta)$ such that $\varepsilon \equiv \pm 1$ modulo $\mathfrak{l} = (1-\zeta)$. Conversely, if ε is such a unit in $k(\zeta)$ and Ω is a root number of the field k then $\Omega^* = \varepsilon\Omega$ is also a root number of k.*

Proof. Under the hypothesis of the first assertion the quotient $\varepsilon = \Omega^*/\Omega$ is a number in the compositum of k and $k(\zeta)$ which remains unaltered when we replace ζ and ν by ζ and $t\nu$ respectively and hence lies in $k(\zeta)$. Let $\omega = \Omega^l$ have the form described in Theorem 135. Let $s^{-a}\mathfrak{p}$ (where a is one of the numbers $0, 1, 2, \dots, l-2$) be that one among the conjugates of the prime ideal divisor of p in k which occurs only to the first power in $\omega^* = (\Omega^*)^l$. Then, according to Theorem 135, we have

$$\omega^* = \mathfrak{p}^{s^{-a}(r_0+r_{-1}s+\cdots+r_{-l+2}s^{l-2})},$$

and it follows from this that the prime ideal $\mathfrak{p}$ occurs in ω^* precisely to the r_{-a}-th power. The quotient ω^*/ω can thus be expressed as a fraction whose numerator is divisible by $\mathfrak{p}^{r_{-a}-r_0}$ and whose denominator is prime to $\mathfrak{p}$. Since $\omega^*/\omega = \varepsilon^l$ the exponent $r_{-a} - r_0$ must be divisible by l; hence $r_{-a} = r_0$ and so $a = 0$. From this it follows that ω and ω^* are products of the same powers of the prime ideal divisors of p; hence ε is a unit.

The remaining assertions of Theorem 137 follow immediately from Theorems 133 and 134.

Using (24.1) we can obtain from the root numbers corresponding to t all the normal bases ν, $t\nu, \dots, t^{l-1}\nu$ of the abelian field k.

§111. The Lagrange Normal Basis and the Lagrange Root Number

Again let l be an odd prime number, $\zeta = e^{2\pi i/l}$ and p a prime number of the form $lm+1$. Let $\mathsf{Z} = e^{2\pi i/p}$ and R be a primitive root modulo p. Let k be the abelian field of degree l with discriminant p^{l-1}.

The $p-1$ numbers $\mathsf{Z}, \mathsf{Z}^2, \dots, \mathsf{Z}^{p-1}$ form a normal basis of the field $k(\mathsf{Z})$. It follows from the proof of Lemma 20 that the l numbers

$$\begin{aligned}
\lambda_0 &= \mathsf{Z} + \mathsf{Z}^{R^l} + \mathsf{Z}^{R^{2l}} + \cdots + \mathsf{Z}^{R^{(m-1)l}}, \\
\lambda_1 &= \mathsf{Z}^R + \mathsf{Z}^{R^{1+l}} + \mathsf{Z}^{R^{1+2l}} + \cdots + \mathsf{Z}^{R^{1+(m-1)l}}, \\
&\cdots\cdots\cdots \\
\lambda_{l-1} &= \mathsf{Z}^{R^{l-1}} + \mathsf{Z}^{R^{2l-1}} + \mathsf{Z}^{R^{3l-1}} + \cdots + \mathsf{Z}^{R^{ml-1}}
\end{aligned}$$

form a normal basis for the field k. From this normal basis we produce the following root number for k:

$$\begin{aligned}
\Lambda &= \lambda_0 + \zeta\lambda_1 + \zeta^2\lambda_2 + \cdots + \zeta^{l-1}\lambda_{l-1} \\
&= \mathsf{Z} + \zeta\mathsf{Z}^R + \zeta^2\mathsf{Z}^{R^2} + \cdots + \zeta^{p-2}\mathsf{Z}^{R^{p-2}}.
\end{aligned}$$

The special normal basis $\lambda_0, \lambda_1, \dots, \lambda_{l-1}$ is called the *Lagrange normal basis* and the root number Λ the *Lagrange root number.*

§112. The Characteristic Properties of the Lagrange Root Number

The Lagrange root number Λ of the field k is distinguished from the other root numbers of k by the following properties.

Theorem 138. *If the l-th power Λ^l of the Lagrange root number Λ is expressed, in accordance with Theorem 135, as*

$$\Lambda^l = \mathfrak{p}^{r_0 + r_{-1}s + r_{-2}s^2 + \cdots + r_{-l+2}s^{l-2}}$$

then the prime ideal $\mathfrak{p}$ is determined by the formula

$$\mathfrak{p} = (p, \zeta - R^{-m}),$$

where $m = (p-1)/l$. The remaining symbols have the same meaning as in Theorem 135. The Lagrange root number Λ is congruent to -1 modulo $\mathfrak{l}$ and its absolute value is $|\sqrt{p}|$.

Conversely, if a root number Ω has these properties and if, further, Ω^l is divisible by precisely the first power of the prime ideal $\mathfrak{p}$ just defined, then

$\Omega = \zeta^* \Lambda$ where ζ^* is an l-th root of unity.

Proof. Let $\mathfrak{P} = (1 - \mathrm{Z}, \mathfrak{p})$. Then, using the relations $(1 - \mathrm{Z})^{p-1} = (p)$ and $(p, \mathfrak{p}^{p-1}) = \mathfrak{p}$, we find that

$$\mathfrak{P}^{p-1} = (p, (1 - \mathrm{Z})^{p-2}\mathfrak{p}, \ldots, \mathfrak{p}^{p-1}) = \mathfrak{p}.$$

From this it is clear that $\mathfrak{P}$ is a prime ideal in the field generated by ζ and Z and that the number $1 - \mathrm{Z}$ is divisible by only the first power of this prime ideal $\mathfrak{P}$. We set $\mathrm{Z} = 1 + \Pi$; and, making use of the congruence $\zeta \equiv R^{-m}$ (mod $\mathfrak{p}$) and the equation $(1 + \Pi)^p = 1$ we find that

$$\begin{aligned} \Lambda &\equiv \sum_{(x)} R^{-mx}(1 + \Pi)^{R^x} \pmod{\mathfrak{p}} \\ &\equiv \sum_{(X)} \Big\{ X^{-m} \sum_{(Y)} \binom{X}{Y} \Pi^Y \Big\} \pmod{\mathfrak{p}} \end{aligned}$$

where the respective sums are taken over $x = 0, 1, 2, \ldots, p-2$; $X = 1, 2, \ldots, p-1$; $Y = 0, 1, 2, \ldots, X$. When we invert the order of summation in the second formula we obtain the congruence

$$\Lambda \equiv -\frac{\Pi^m}{m!} \pmod{\mathfrak{P}^{m+1}}. \tag{24.4}$$

The Lagrange root number is thus divisible by precisely the m-th power of $\mathfrak{P}$ and consequently Λ^l is divisible only by the first power of $\mathfrak{p}$.

If we denote the complex conjugate of Λ by $\bar{\Lambda}$ we have

$$\bar{\Lambda} = \mathrm{Z}^{-1} + \zeta^{-1}\mathrm{Z}^{-R} + \zeta^{-2}\mathrm{Z}^{-R^2} + \cdots + \zeta^{-p+2}\mathrm{Z}^{-R^{p-2}};$$

when we form the product $\Lambda\bar{\Lambda}$ and collect the terms involving the same power of ζ we obtain

$$\begin{aligned} \Lambda\bar{\Lambda} &= (1 + 1 + \cdots + 1) \\ &\quad + \zeta(\mathrm{Z}^{R-1} + \mathrm{Z}^{R^2-R} + \cdots + \mathrm{Z}^{R^{p-1}-R^{p-2}}) \\ &\quad + \zeta^2(\mathrm{Z}^{R^2-1} + \mathrm{Z}^{R^3-R} + \cdots + \mathrm{Z}^{R^p-R^{p-2}}) \\ &\quad + \ldots\ldots \\ &\quad + \zeta^{p-2}(\mathrm{Z}^{R^{p-2}-1} + \mathrm{Z}^{R^{p-1}-R} + \cdots + \mathrm{Z}^{R^{2p-4}-R^{p-2}}) \\ &= p - 1 - (\zeta + \zeta^2 + \cdots + \zeta^{p-2}) = p \end{aligned}$$

This establishes the first part of Theorem 138.

The second part is essentially the converse of the first. It follows easily from Theorems 135 and 137 when we make use also of Theorem 48; we have to take account of the fact that when a number of an abelian field has absolute value 1 then so also do all its conjugates.

By arguments similar to those used for (24.4) we can also deduce the following congruences (*Jacobi* (3)):

$$s^{-i}\Lambda \equiv -\frac{\Pi^{r_{-i}m}}{(r_{-i}m)!} \pmod{\mathfrak{P}^{r_{-i}m+1}} \tag{24.5}$$

for $i = 0, 1, 2, \ldots, l-2$. If we bear in mind that Λ is congruent to -1 modulo l and that $|\Lambda| = |\sqrt{p}|$ we can obtain from the congruences (24.5) another proof of Theorems 135 and 136 (*Kummer* (6, 11)).

All the theorems and proofs in this chapter hold also for $l = 2$ except that in that case the discriminant of the abelian field k takes the value $d = (-1)^{\frac{1}{2}(p-1)}p$.

The Lagrange root number Λ of the field k is an integer of the compositum of k and $k(\zeta)$ which, according to the properties enumerated in Theorems 133 and 138, is completely determined up to the factor ζ^*. Finally, in order to determine ζ^* we must set $\Lambda = |\sqrt{p}|e^{2\pi i\varphi}$, where $0 \leq \varphi < 1$, and then discover which of the intervals

$$0 \leq \varphi < \frac{1}{l}, \frac{1}{l} \leq \varphi < \frac{2}{l}, \ldots, \frac{l-1}{l} \leq \varphi < 1$$

contains the required number φ. In the case where instead of l we take the prime number 2 this question gives rise to the celebrated problem of the determination of the sign of the Gauss sum (cf Sect. 124). For the case $l = 3$ we are led to a problem tackled by Kummer (*Kummer* (2, 4)).

The numbers of the Lagrange normal basis are usually called "periods", The literature includes a collection of articles concerned with these periods and related integers in cyclotomic fields (*Kummer* (3, 17), *Fuchs* (1, 2), *Schwering* (1, 3, 4), *Kronecker* (17), *Smith* (1)). In the literature we find also investigations into particular cyclotomic fields (*Berkenbusch* (1), *Eisenstein* (10), *Schwering* (2), *Weber* (1, 2, 4), *Wolfskehl* (1)). We mention here also that if the prime number l is less than 100 and not equal to 29 or 41 then the cyclotomic field $k(\zeta)$ always has an ideal class whose powers constitute all the classes of the field (*Kummer* (11, 13)).

25. The Reciprocity Law for l-th Power Residues Between a Rational Number and a Number in the Field of l-th Roots of Unity

§113. The Power Character of a Number and the Symbol $\left\{\frac{\alpha}{\mathfrak{p}}\right\}$

Let l be an odd prime number, $\zeta = e^{2\pi i/l}$ and $k(\zeta)$ the cyclotomic field generated by ζ. Let p be a rational prime number distinct from l and $\mathfrak{p}$ a prime ideal of $k(\zeta)$ dividing p. If $\mathfrak{p}$ has degree f then, according to Theorem 24, we have for every integer α of $k(\zeta)$ not divisible by $\mathfrak{p}$ the congruence

$$\alpha^{p^f-1} - 1 \equiv 0 \pmod{\mathfrak{p}}.$$

By Theorem 119 $p^f - 1$ is divisible by l; so the left hand side of this congruence admits the factorisation

$$\alpha^{p^f-1} - 1 = \prod_{(c)} (\alpha^{(p^f-1)/l} - \zeta^c)$$

where the product is taken over the range $c = 0, 1, \ldots, l-1$. From this it follows that for one (and in fact only one) value of c we have the congruence

$$\alpha^{(p^f-1)/l} \equiv \zeta^c \pmod{\mathfrak{p}}.$$

The root of unity ζ^c which appears here is called the *power character* of the number α with respect to the prime ideal $\mathfrak{p}$ in $k(\zeta)$ and we denote this root of unity ζ^c by the symbol $\left\{\frac{\alpha}{\mathfrak{p}}\right\}$; so we have (*Kummer* (10))

$$\alpha^{p^f-1} - 1 \equiv \left\{\frac{\alpha}{\mathfrak{p}}\right\} \pmod{\mathfrak{p}}. \tag{25.1}$$

If α and β are two integers of $k(\zeta)$ not divisible by $\mathfrak{p}$ then it follows easily that

$$\left\{\frac{\alpha\beta}{\mathfrak{p}}\right\} = \left\{\frac{\alpha}{\mathfrak{p}}\right\}\left\{\frac{\beta}{\mathfrak{p}}\right\}.$$

If in particular the integer α is congruent modulo $\mathfrak{p}$ to the l-th power of an

integer in $k(\zeta)$ we call α an *l-th power residue* modulo the prime ideal $\mathfrak{p}$. We have the following result.

Theorem 139. *If $\mathfrak{p}$ is a prime ideal of $k(\zeta)$ distinct from $\mathfrak{l} = (1-\zeta)$ and α is an integer of $k(\zeta)$ prime to $\mathfrak{p}$ then α is an l-th power residue modulo $\mathfrak{p}$ if and only if $\left\{\frac{\alpha}{\mathfrak{p}}\right\} = 1$.*

Proof. Suppose $\alpha \equiv \beta^l \pmod{\mathfrak{p}}$, where β is an integer of $k(\zeta)$. Then we have $\alpha^{(p^f-1)/l} \equiv \beta^{p^f-1} \equiv 1 \pmod{\mathfrak{p}}$ and so $\left\{\frac{\alpha}{\mathfrak{p}}\right\} = 1$. To prove the converse, let ρ be a primitive root modulo $\mathfrak{p}$ and set $\alpha \equiv \rho^h \pmod{\mathfrak{p}}$. If we have $\alpha^{(p^f-1)/l} \equiv \rho^{h(p^f-1)/l} \equiv 1 \pmod{\mathfrak{p}}$ it follows that

$$\frac{h(p^f-1)}{l} \equiv 0 \pmod{p^f-1},$$

i.e. that h is divisible by l and so α is an l-th power residue modulo $\mathfrak{p}$ as asserted.

If ρ is a primitive root modulo $\mathfrak{p}$ the power character $\left\{\frac{\rho}{\mathfrak{p}}\right\}$ is certainly not equal to 1. For in the sequence $\rho, \rho^2, \ldots$ the first number congruent to 1 modulo $\mathfrak{p}$ is ρ^{p^f-1} and hence $\rho^{(p^f-1)/l} \not\equiv 1 \pmod{\mathfrak{p}}$.

Suppose $\left\{\frac{\rho}{\mathfrak{p}}\right\} = \zeta^g$; let g^* be a rational integer prime to p^f-1 such that $gg^* \equiv 1 \pmod{l}$. Then $\rho^* = \rho^{g^*}$ is clearly a primitive root modulo $\mathfrak{p}$ for which we have $\left\{\frac{\rho^*}{\mathfrak{p}}\right\} = \zeta$. If now α is any integer of $k(\zeta)$ not divisible by $\mathfrak{p}$ and $\alpha \equiv (\rho^*)^c \pmod{\mathfrak{p}}$ then the power character of α is ζ^c.

From this it follows easily that the complete set of numbers $1, \rho^*, (\rho^*)^2, \ldots, (\rho^*)^{p^f-2}$ mutually incongruent modulo $\mathfrak{p}$ splits into l subsets such that all $(p^f-1)/l$ members of each subset have the same power character. In particular there are $(p^f-1)/l$ mutually incongruent l-th power residues modulo $\mathfrak{p}$.

If $\mathfrak{b}$ is any ideal of $k(\zeta)$ prime to $\mathfrak{l}$ and α is an integer of $k(\zeta)$ prime to $\mathfrak{b}$ then, if $\mathfrak{b} = \mathfrak{p}\mathfrak{q}\cdots\mathfrak{w}$ where $\mathfrak{p}, \mathfrak{q}, \ldots, \mathfrak{w}$ are prime ideals, the symbol $\left\{\frac{\alpha}{\mathfrak{b}}\right\}$ is defined by the equation

$$\left\{\frac{\alpha}{\mathfrak{b}}\right\} = \left\{\frac{\alpha}{\mathfrak{p}}\right\}\left\{\frac{\alpha}{\mathfrak{q}}\right\}\cdots\left\{\frac{\alpha}{\mathfrak{w}}\right\}.$$

§114. A Lemma on the Power Character of the l-th Power of the Lagrange Root Number

Eisenstein succeeded in discovering and proving the reciprocity law which subsists in $k(\zeta)$ between a rational number and an arbitrary number of this

field. (Here again we take ζ to be $e^{2\pi i/l}$ where l is an odd prime number.) This reciprocity law is also a tool which has hitherto been found indispensable in the proof of the general Kummer reciprocity law (cf Chap. 31). For the proof of the Eisenstein reciprocity law we need the following lemma.

Lemma 21. *Let $\zeta = e^{2\pi i/l}$; let p be a rational prime number distinct from l of the form $ml+1$; let R be a primitive root modulo p and $\mathfrak{p}$ the prime ideal $(p, \zeta - R^{-m})$ of degree 1 in $k(\zeta)$. Let $\mathsf{Z} = e^{2\pi i/p}$ and*

$$\Lambda = \mathsf{Z} + \zeta \mathsf{Z}^{R} + \zeta^2 \mathsf{Z}^{R^2} + \cdots + \zeta^{p-2}\mathsf{Z}^{R^{p-2}}$$

the Lagrange root number; set $\pi = \Lambda^l$. Finally let q be a rational prime number distinct from p and l; let $\mathfrak{q}$ be a prime ideal of $k(\zeta)$ which divides q and let g be the degree of $\mathfrak{q}$. Then the power character of the number $\pi = \Lambda^l$ with respect to the ideal $\mathfrak{q}$ is given by the formula

$$\left\{\frac{\pi}{\mathfrak{q}}\right\} = \left\{\frac{q}{\mathfrak{p}}\right\}^g.$$

Proof. By raising the equation for Λ to the q-th power g times we have the congruence

$$\Lambda^{q^g} \equiv \mathsf{Z}^{q^g} + \zeta^{q^g}\mathsf{Z}^{Rq^g} + \zeta^{2q^g}\mathsf{Z}^{R^2q^g} + \cdots + \zeta^{(p-2)q^g}\mathsf{Z}^{R^{p-2}q^g} \pmod{q}. \quad (25.2)$$

If we recall that according to Theorem 119 we have $q^g \equiv 1 \pmod{l}$ and write $q^g \equiv R^h \pmod{p}$ then the right hand side of the congruence (25.2) becomes

$$\mathsf{Z}^{R^h} + \zeta\mathsf{Z}^{R^{h+1}} + \zeta^2\mathsf{Z}^{R^{h+2}} + \cdots + \zeta^{p-2}\mathsf{Z}^{R^{h+p-2}} = \zeta^{-h}\Lambda.$$

From this, since (by Theorem 138) Λ is prime to q, we have the congruence

$$\Lambda^{q^g-1} \equiv \zeta^{-h} \pmod{q}$$

and from this we deduce that

$$\Lambda^{q^g-1} = \pi^{q^g-1/l} \equiv \zeta^{-h} \pmod{\mathfrak{q}}$$

and hence

$$\left\{\frac{\pi}{\mathfrak{q}}\right\} = \zeta^{-h}. \quad (25.3)$$

On the other hand we deduce from the congruences $q^g \equiv R^h \pmod{p}$ and $R^m \equiv \zeta^{-1} \pmod{\mathfrak{p}}$ that

$$q^{g(p-1)/l} = q^{gm} \equiv R^{hm} \equiv \zeta^{-h} \pmod{\mathfrak{p}}.$$

Thus we have

$$\left\{\frac{q^g}{\mathfrak{p}}\right\} = \left\{\frac{q}{\mathfrak{p}}\right\}^g = \zeta^{-h}. \quad (25.4)$$

Equations (25.3) and (25.4) together yield the result of Lemma 21.

§115. Proof of the Reciprocity Law in the Field $k(\zeta)$ Between a Rational Number and an Arbitrary Number

Let $\mathfrak{l} = (1-\zeta)$ be the prime ideal of the field $k(\zeta)$ which divides l. An integer α of $k(\zeta)$ is called *semiprimary* if it is prime to $\mathfrak{l}$ and congruent modulo $\mathfrak{l}^2$ to a rational integer; according to this definition every rational integer not divisible by l is semiprimary. Any integer α of the field $k(\zeta)$ can be transformed into a semiprimary number by multiplying by a suitable power of ζ. In fact, if

$$\alpha \equiv a + b(1-\zeta) \pmod{\mathfrak{l}^2},$$

where a and b are rational integers, we have

$$\zeta^{b^*} \cdot \alpha \equiv a \pmod{\mathfrak{l}^2},$$

where b^* is determined by the congruence $ab^* \equiv b \pmod{l}$. Thus the number $\zeta^{b^*}\alpha$ is semiprimary.

After this introduction we can now state the *Eisenstein reciprocity law* as follows.

Theorem 140. *Let a be a rational integer not divisible by the odd prime number l and α a semiprimary number prime to a in the field $k(\zeta)$ of the l-th roots of unity. Then in this field we have the reciprocity equation*

$$\left\{\frac{a}{\alpha}\right\} = \left\{\frac{\alpha}{a}\right\}$$

(*Eisenstein* (2)).

Proof. We let r be a primitive root modulo l and write $s = (\zeta : \zeta^r)$.

We suppose first that a is a rational prime number, q say, and that the number α is divisible only by prime ideals of $k(\zeta)$ of degree 1. Let $\mathfrak{q}$ be a prime ideal of $k(\zeta)$ dividing q; let g be the degree of $\mathfrak{q}$. Let p be a rational prime dividing the norm $n(\alpha)$ and let π and $\mathfrak{p}$ have the same meaning as in Lemma 21. If s^u is any power of the automorphism s then, applying Lemma 21 to the prime ideals $s^{-u}\mathfrak{q}$ and $\mathfrak{p}$, we have

$$\left\{\frac{\pi}{s^{-u}\mathfrak{q}}\right\} = \left\{\frac{q}{\mathfrak{p}}\right\}^g.$$

Applying the automorphism s^u to this equation, we obtain

$$\left\{\frac{s^u\pi}{\mathfrak{q}}\right\} = \left\{\frac{q}{s^u\mathfrak{p}}\right\}^g. \tag{25.5}$$

Let the distinct rational primes dividing the norm $n(\alpha)$ be $p = ml+1$, $p^* = m^*l+1, \ldots$; let $R, R^*, \ldots$ be primitive roots modulo $p, p^*, \ldots$ respectively; set

$$\mathfrak{p} = (p, \zeta - R^{-m}), \mathfrak{p}^* = (p^*, \zeta - (R^*)^{-m}), \ldots$$

and suppose α splits as

$$\alpha = \mathfrak{p}^{F(s)}(\mathfrak{p}^*)^{F^*(s)} \ldots$$

where the exponents F, F^*, are all polynomials in s of degree $l-2$ all of whose coefficients are non-negative integers.

Let Λ, Λ^*, ... be the Lagrange root numbers corresponding respectively to the primes p, p^*, ... and their primitive roots R, R^*, ...; set $\pi = \Lambda^l$, $\pi^* = (\Lambda^*)^l$, ... Then, according to Theorem 138, we have

$$\begin{aligned} \pi &= \mathfrak{p}^{r_0+r_{-1}s+r_{-2}s^2+\cdots+r_{-l+2}s^{l-2}}, \\ \pi^* &= (\mathfrak{p}^*)^{r_0+r_{-1}s+r_{-2}s^2+\cdots+r_{-l+2}s^{l-2}}, \\ &\ldots\ldots \end{aligned}$$

where r_{-h} is the least positive rational integer congruent modulo l to the $(-h)$-th power r^{-h} of the primitive root r. The quotient

$$\varepsilon = \frac{\alpha^{r_0+r_{-1}s+r_{-2}s^2+\cdots+r_{-l+2}s^{l-2}}}{\pi^{F(s)}(\pi^*)^{F^*(s)}\ldots}$$

is then clearly a unit of the field $k(\zeta)$. We shall prove that this unit $\varepsilon = \pm 1$. To this end we form the expression

$$|\varepsilon|^2 = \varepsilon^{1+s^{\frac{1}{2}(l-1)}} = \frac{\alpha^{(1+s^{\frac{1}{2}(l-1)})(r_0+r_{-1}s+r_{-2}s^2+\cdots+r_{-l+2}s^{l-2})}}{(|\pi|^2)^{F(s)}(|\pi^*|^2)^{F^*(s)}\ldots}.$$

For $h = 0, 1, 2, \ldots, \frac{1}{2}(l-3)$ we have the equations

$$r_{-h} + r_{-h-\frac{1}{2}(l-1)} = l;$$

so the numerator of the fraction on the right hand side is

$$\alpha^{(1+s^{\frac{1}{2}(l-1)})(r_0+r_{-1}s+r_{-2}s^2+\cdots+r_{-l+2}s^{l-2})} = \alpha^{l(1+s+\cdots+s^{l-2})} = (n(\alpha))^l.$$

Bearing in mind that, according to Theorem 138, we have $|\pi|^2 = p^l$, $|\pi^*|^2 = (\mathfrak{p}^*)^l$, ..., we deduce that $|\varepsilon| = 1$. It follows from Theorem 48 that ε is (up to a factor of ± 1) a power of the root of unity ζ. Since on the other hand (by Theorem 138) we have the congruences

$$\pi \equiv -1, \quad \pi^* \equiv -1, \ldots \quad (\text{mod } \mathfrak{l}^l),$$

so that π, π^*, ... are all semiprimary numbers, it follows that ε is also a semiprimary number. Hence $\varepsilon = \pm 1$ and consequently

$$\alpha^{r_0+r_{-1}s+r_{-2}s^2+\cdots+r_{-l+2}s^{l-2}} = \pm\pi^{F(s)}(\pi^*)^{F^*(s)}\ldots$$

When we apply formula (25.5) this equation yields the reciprocity equation

$$\left\{\frac{\alpha^{r_0+r_{-1}s+\cdots+r_{-l+2}s^{l-2}}}{\mathfrak{q}}\right\} = \left\{\frac{q}{\mathfrak{p}^{F(s)}(\mathfrak{p}^*)^{F^*(s)}\cdots}\right\}^g = \left\{\frac{q}{\alpha}\right\}^g. \tag{25.6}$$

We notice that

$$\left\{\frac{s\alpha}{\mathfrak{q}}\right\} = \left\{\frac{\alpha}{s^{-1}\mathfrak{q}}\right\}^r, \left\{\frac{s^2\alpha}{\mathfrak{q}}\right\} = \left\{\frac{\alpha}{s^{-2}\mathfrak{q}}\right\}^{r^2}, \ldots, \left\{\frac{s^{l-2}\alpha}{\mathfrak{q}}\right\} = \left\{\frac{\alpha}{s^{-l+2}\mathfrak{q}}\right\}^{r^{l-2}};$$

then, since the symbols are powers of ζ, we deduce from (25.6) that

$$\left\{\frac{\alpha}{q^g}\right\} = \left\{\frac{q}{\alpha}\right\}^g \quad \text{or} \quad \left\{\frac{\alpha}{q}\right\} = \left\{\frac{q}{\alpha}\right\};$$

thus Theorem 140 is established under the conditions we imposed at the beginning, namely that the prime ideal factors of α are all of degree 1 and that a is a prime number q.

To remove the first restriction we now suppose that α is any semiprimary integer in $k(\zeta)$ prime to q which may be divisible by prime ideals of degree greater than 1. We form the number

$$\beta = \alpha^{\prod_{(e)}(1-s^e)},$$

where the product in the exponent is taken over all the divisors e of $l-1$ apart from $l-1$, and we set

$$\beta = \frac{\mathfrak{i}}{\mathfrak{k}},$$

where $\mathfrak{i}$ and $\mathfrak{k}$ are relatively prime ideals. It is easy to see that $\mathfrak{i}$ and $\mathfrak{k}$ have only prime ideals of degree 1 as factors and that they are not divisible by $\mathfrak{l}$. If h is the number of ideal classes in $k(\zeta)$ then it follows from Theorem 51 that $\mathfrak{k}^h = (\kappa)$ where κ is an integer in $k(\zeta)$. Set $\gamma = \beta\kappa^l$; then γ is an integer of $k(\zeta)$ which has only prime ideals of degree 1 as factors and furthermore, like α, is semiprimary and prime to q. According to the result proved above it follows that

$$\left\{\frac{\gamma}{q}\right\} = \left\{\frac{q}{\gamma}\right\}. \tag{25.7}$$

To simplify the notation we shall now write

$$\frac{\left\{\frac{\rho}{q}\right\}}{\left\{\frac{\sigma}{q}\right\}} = \left\{\frac{\frac{\rho}{\sigma}}{q}\right\} \quad \text{and} \quad \frac{\left\{\frac{q}{\rho}\right\}}{\left\{\frac{q}{\sigma}\right\}} = \left\{\frac{q}{\frac{\rho}{\sigma}}\right\}$$

where ρ and σ are any integers of $k(\zeta)$ prime to q. (This does not conflict with our earlier notation.) Since $\beta = \gamma/\kappa^l$ we deduce from (25.7) that

$$\left\{\frac{\beta}{q}\right\} = \left\{\frac{q}{\beta}\right\}. \tag{25.8}$$

When we take into account the equations

$$\left\{\frac{s^u\alpha}{q}\right\} = \left\{\frac{\alpha}{q}\right\}^{r^u} \quad \text{and} \quad \left\{\frac{q}{s^u\alpha}\right\} = \left\{\frac{q}{\alpha}\right\}^{r^u},$$

we deduce from (25.8) that

$$\left\{\frac{\alpha}{q}\right\}^{\prod_{(e)}(1-r^e)} = \left\{\frac{q}{\alpha}\right\}^{\prod_{(e)}(1-r^e)}.$$

If we notice that the product which occurs as exponent on both sides is not divisible by l then we obtain

$$\left\{\frac{\alpha}{q}\right\} = \left\{\frac{q}{\alpha}\right\}.$$

Finally suppose that a is an arbitrary rational integer not divisible by l, subject only to the condition that it is prime to α. If we set $a = qq^* \cdots$, where q, q^*, ... are rational primes, then multiplication of the equations

$$\left\{\frac{\alpha}{q}\right\} = \left\{\frac{q}{\alpha}\right\} \quad \text{and} \quad \left\{\frac{\alpha}{q^*}\right\} = \left\{\frac{q^*}{\alpha}\right\}, \ldots$$

yields the result of Theorem 140 in the most general case.

26. Determination of the Number of Ideal Classes in the Cyclotomic Field of the m-th Roots of Unity

§116. The Symbol $\left[\frac{a}{L}\right]$

In order to apply the transcendental method described in Sect. 26 for finding the class number of a field to the case of the cyclotomic field $k(e^{2\pi i/m})$ where m is a rational integer we introduce first the following symbols.

Let l^h be a power with positive exponent of an odd prime l and r a primitive root modulo l^h. If a is a rational integer not divisible by l and a' an exponent such that

$$r^{a'} \equiv a \pmod{l^h}$$

then we define

$$\left[\frac{a}{l^h}\right] = e^{2\pi i a'/l^{h-1}(l-1)}.$$

In addition we set

$$\left[\frac{a}{l^h}\right] = 0$$

if a is divisible by l. If a and b are any rational integers then clearly

$$\left[\frac{ab}{l^h}\right] = \left[\frac{a}{l^h}\right]\left[\frac{b}{l^h}\right].$$

If a is an odd integer then we define

$$\left[\frac{a}{2^2}\right] = (-1)^{\frac{1}{2}(a-1)}$$

and, for an exponent h greater than 2, if a' is a rational integer such that

$$5^{a'} \equiv \pm a \pmod{2^h},$$

we set

$$\left[\frac{a}{2^h}\right] = e^{2\pi i a'/2^{h-2}}.$$

Finally, if a is an even number, we set

$$\left[\frac{a}{2^2}\right] = 0 \quad \text{and} \quad \left[\frac{a}{2^2}\right] = 0 \quad (h > 2).$$

If a and b are any rational integers it is easy to see that

$$\left[\frac{ab}{2^h}\right] = \left[\frac{a}{2^h}\right]\left[\frac{b}{2^h}\right] \quad (h > 1).$$

According to these definitions the symbol $\left[\frac{a}{L}\right]$ is completely determined for the cases where a is any rational integer and L is either a power of 2 higher than the first or else any power of an odd prime, where in the latter case a particular primitive root r modulo L is fixed in advance.

Let $l_1^{h_1}$, $l_2^{h_2}$, ... be given powers of distinct odd primes and 2^{h^*} a power of 2 greater than 2^2. Then for brevity we set

$$\left[\frac{a}{\overbrace{u_1, u_2, \ldots}}\right] = \left[\frac{a}{l_1^{h_1}}\right]^{u_1}\left[\frac{a}{l_2^{h_2}}\right]^{u_2}\cdots,$$

$$\left[\frac{a}{\overbrace{u; u_1, u_2, \ldots}}\right] = \left[\frac{a}{2^2}\right]^{u}\left[\frac{a}{l_1^{h_1}}\right]^{u_1}\left[\frac{a}{l_2^{h_2}}\right]^{u_2}\cdots,$$

$$\left[\frac{a}{\overbrace{u, u^*; u_1, u_2, \ldots}}\right] = \left[\frac{a}{2^2}\right]^{u}\left[\frac{a}{2^{h^*}}\right]^{u^*}\left[\frac{a}{l_1^{h_1}}\right]^{u_1}\left[\frac{a}{l_2^{h_2}}\right]^{u_2}\cdots,$$

where a is any rational integer and u, u^*; u_1, u_2, ... are non-negative rational integers. Finally we stipulate that $\left[\frac{a}{L}\right]^0$ shall always have the value 1 even when $\left[\frac{a}{L}\right] = 0$.

§117. The Expression for the Class Number of the Cyclotomic Field of the m-th Roots of Unity

We state the following theorem, whose proof will be given in Sect. 118.

Theorem 141. *Let m be a positive rational integer of the form*

$$m = l_1^{h_1} l_2^{h_2}\cdots \quad \text{or} \quad m = 2^2 l_1^{h_1} l_2^{h_2}\cdots \quad \text{or} \quad m = 2^{h^*} l_1^{h_1} l_2^{h_2}\cdots$$

$$(h^* > 2, h_1 > 0, h_2 > 0, \ldots).$$

where l_1, l_2, ... are distinct odd primes. Let r_1, r_2, ... be primitive roots modulo $l_1^{h_1}$, $l_2^{h_2}$, ... respectively and use them to define the corresponding symbols. Then the class number H of the cyclotomic field k of the m-th roots of unity can be expressed in two ways as described below.

(1) The first form for H is as follows:

$$H = \frac{1}{\kappa} \prod_{(u_1,u_2,\dots)} \lim_{s=1} \prod_{(p)} \frac{1}{1 - \left[\overbrace{\frac{p}{u_1, u_2, \dots}}\right] p^{-s}}$$

when $m = l_1^{h_1} l_2^{h_2} \cdots$ and $u_1, u_2, \dots$ are replaced by $u; u_1, u_2, \dots$ and by $u, u^*; u_1, u_2, \dots$ when $m = 2^2 l_1^{h_1} l_2^{h_2} \cdots$ and $m = e^{h^*} l_1^{h_1} l_2^{h_2} \cdots$ respectively. The outer product is taken over the ranges

$$\left.\begin{array}{rcl} u_1 &=& 0, 1, \dots, l_1^{h_1 - 1}(l_1 - 1) - 1, \\ u_2 &=& 0, 1, \dots, l_1^{h_2 - 1}(l_2 - 1) - 1, \\ & & \dots\dots\dots \\ u &=& 0, 1 \\ u^* &=& 0, 1, \dots, 2^{h^* - 2} - 1 \end{array}\right\} \tag{26.1}$$

excluding the combinations $u_1 = u_2 = \dots = 0$, $u = u_1 = u_2 = \dots = 0$, $u = u^* = u_1 = u_2 = \dots = 0$ respectively. So the outer product consists of a finite number of factors. Each inner product $\prod\limits_{(p)}$ runs over all the rational prime numbers p and hence is an infinite product. The number κ is the number associated to the field in Theorem 56 (see p. 60).

(2) The second expression for H is a product of two factors, each of which is a fraction: in the first case

$$H = \frac{\prod\limits_{(u_1,u_2,\dots)} \sum\limits_{(n)} \left[\overbrace{\frac{n}{u_1, u_2, \dots}}\right] n}{(2m)^{\frac{1}{2}\Phi(m)-1}} \cdot \frac{\prod\limits_{(u_1,u_2,\dots)} \sum\limits_{(n)} \left[\overbrace{\frac{n}{u_1, u_2, \dots}}\right] \log \mathsf{A}_n}{R} 2^{\frac{1}{2}\Phi(m)-1};$$

in the other cases the first fraction on the right hand side has the additional factor $\frac{1}{2}$ and u_1, u_2, ... are replaced by u; u_1, u_2, ... or u, u^*; u_1, u_2, ... respectively. Here the product $\prod$ in the numerator of the first fraction runs over all the numbers given in (26.1) for which, in the first case, $u_1 + u_2 + \dots$ and, in the other two cases, $u + u_1 + u_2 + \dots$ is an odd number while the product $\prod$ in the numerator of the second fraction is taken over all the numbers in (26.1) for which in the first case $u_1 + u_2 + \cdots$ and in the other two cases $u + u_1 + u_2 + \cdots$ is an even number (excluding always the combinations $u_1 = u_2 = \dots = 0$; $u = u_1 = u_2 = \dots = 0$; $u = u^* = u_1 = u_2 = \dots = 0$ in the three cases respectively). Each sum $\sum\limits_{(n)}$ in the first fraction extends over all positive rational integers $n = 1, 2, \dots, m-1$ and each sum $\sum\limits_{(n)}$ in the second fraction only over all those integers which are less than $\frac{1}{2}m$. Finally $\log \mathsf{A}_n$ denotes the real value of the logarithm of the cyclotomic number

$$\mathsf{A}_n = \sqrt{(1 - e^{2\pi in/m})(1 - e^{-2\pi in/m})}$$

and R is the regulator of the cyclotomic field (*Kummer* (22, 23)).

Kummer called the two fractions appearing in the second expression for H the *first* and *second factors* of the class number. Twice the first factor and the second factor are rational integers (*Kronecker* (9)).

Using the second expression for H Weber proved that the class number of the cyclotomic field of the 2^{h^*}-th roots of unity is always an odd number (*Weber* (1, 4)).

The second expression for H can be further transformed. In the case where $m = l$ is an odd prime number an easy calculation produces the following result.

Theorem 142. *Let l be an odd prime number. Then the class number h of the cyclotomic field of the l-th roots of unity is given by the expression*

$$h = \frac{\prod\limits_{(u)} \sum\limits_{(n)} n e^{2\pi in'u/(l-1)}}{(2l)^{\frac{1}{2}(l-3)}} \cdot \frac{\Delta}{R} 2^{\frac{1}{2}(l-3)},$$

where the product $\prod\limits_{(u)}$ is taken over the odd numbers $u = 1, 3, 5, \ldots, l-2$ and each sum $\sum\limits_{(n)}$ is taken over the range $n = 1, 2, 3, \ldots, l-1$. A primitive root r modulo l is chosen and for each n we determine n' such that $r^{n'} \equiv n \pmod{l}$. Δ is the determinant

$$(-1)^{(l-3)(l-5)/8} \begin{vmatrix} \log \varepsilon_1 & \log \varepsilon_2 & \cdots & \log \varepsilon_{\frac{1}{2}(l-3)} \\ \log \varepsilon_2 & \log \varepsilon_3 & \cdots & \log \varepsilon_{\frac{1}{2}(l-1)} \\ & & \cdots\cdots & \\ \log \varepsilon_{\frac{1}{2}(l-3)} & \log \varepsilon_{\frac{1}{2}(l-1)} & \cdots & \log \varepsilon_{l-4} \end{vmatrix}$$

where in general $\log \varepsilon_g$ is the real value of the logarithm of the unit

$$\varepsilon_g = \sqrt{\frac{1 - \zeta^{r^g}}{1 - \zeta^{r^{g-1}}} \cdot \frac{1 - \zeta^{-r^g}}{1 - \zeta^{-r^{g-1}}}}$$

where $\zeta = e^{2\pi i/l}$ (Kummer (7, 11), Dedekind (1)).

The two fractions occurring in this expression for h arise from the two fractions in the formula given above for the general case and hence are the first and second factors of the class number in the earlier sense. In the present case both factors of the class number are rational integers. The second factor represents the class number of the real subfield of $k(\zeta)$ of degree $\frac{1}{2}(l-1)$. Kummer has stated other results about these two factors concerned with their divisibility by 2 (*Kummer* (25)). The attempts by Kronecker to prove

these theorems by purely arithmetic means contain a mistake and the generalisation given by Kronecker is not correct (*Kronecker* (11)). In addition Kummer has carried out investigations in another direction into the meaning and properties of these two factors (*Kummer* (13)). We refer also to Chap. 36. Finally, Kummer has stated a result asserting that the class number of every subfield of $k(\zeta)$ is a factor of the class number of $k(\zeta)$. His proof of this statement, however, is not valid (*Kummer* (7)).

§118. Derivation of the Expressions for the Class Number of the Cyclotomic Field $k(e^{2\pi i/m})$

To prove Theorem 141 we consider the most complicated case, in which m is divisible by 8, and state the following lemma.

Lemma 22. *Let p be a rational prime number, m an integer divisible by 8. Then, with the notation introduced in Theorem 141, we have, for all real numbers s greater than 1,*

$$\prod_{(\mathfrak{P})} \{1 - n(\mathfrak{P})^{-s}\} = \prod_{(u,u^*;u_1,u_2,\ldots)} \left\{1 - \left[\frac{p}{\underbrace{u, u^*; u_1, u_2, \ldots}}\right] p^{-s}\right\},$$

where the product on the left hand side is taken over all prime ideals $\mathfrak{P}$ of the cyclotomic field $k(e^{2\pi i/m})$ dividing p and the product on the right hand side over all the ranges for u, u^*; u_1, u_2, ... given in (26.1) (*the system $u = u^* = u_1 = u_2 = \ldots = 0$ being included*).

Proof. First suppose that p is a prime number not dividing m. Let l be one of the odd prime numbers $l_1, l_2, \ldots$ and l^h the exact power of l dividing m; let r be a primitive root modulo l^h and suppose that $p \equiv r^{p'} \pmod{l^h}$. Let e be the greatest common divisor of p' and $l^{h-1}(l-1)$ and $f = l^{h-1}(l-1)/e$. Then the symbol $\left[\frac{p}{l^h}\right]$ is obviously precisely an f-th root of unity (i.e. not a root of unity of lower order).

Choose first $l = l_1$ and correspondingly $h = h_1$, $e = e_1$ and set $f_1 = l_1^{h_1-1}(l_1 - 1)/e_1$. Then we have the formula

$$\prod_{(u_1)} \left\{1 - \left[\frac{p}{\underbrace{u, u^*; u_1, u_2, \ldots}}\right] p^{-s}\right\} = \left\{1 - \left[\frac{p}{\underbrace{u, u^*; u_2, u_3, \ldots}}\right]^{f_1} p^{-sf_1}\right\}^{e_1},$$

where the product extends over the range of u_1 given in (26.1). Next choose $l = l_2$ and correspondingly $h = h_2$, $e = e_2$, $f_1 = l_2^{h_2-1}(l_2 - 1)/e_2$. Then, if f_{12} is the least common multiple of f_1 and f_2, we have

$$\prod_{(u_1,u_2)}\left\{1-\left[\frac{p}{\overbrace{u,u^*;u_1,u_2,\ldots}}\right]p^{-s}\right\}=$$

$$\left\{1-\left[\frac{p}{\overbrace{u,u^*;u_3,u_4,\ldots}}\right]^{f_{12}}p^{-sf_{12}}\right\}^{e_1e_2f_1f_2/f_{12}}$$

where the product is taken over the ranges of u_1, u_2 given in (26.1). Proceeding in this way we obtain, if $f_{12\ldots}$ is the least common multiple of $f_1, f_2, \ldots,$

$$\prod_{(u_1,u_2,\ldots)}\left\{1-\left[\frac{p}{\overbrace{u,u^*;u_1,u_2,\ldots}}\right]p^{-s}\right\}=$$

$$\left\{1-\left[\frac{p}{\overbrace{u,u^*}}\right]^{f_{12\ldots}}p^{-sf_{12\ldots}}\right\}^{e_1e_2\ldots f_1f_2\ldots/f_{12\ldots}},$$

where the product runs over the ranges of u_1, u_2, ... given in (26.1).

Next let $p \equiv \pm 5^{p'} \pmod{2^{h^*}}$; let e^* be the greatest common divisor of p' and 2^{h^*-2}; set $f^* = 2^{h^*-2}/e^*$. Then $\left[\frac{p}{2^{h^*}}\right]$ is precisely an f^*-th root of unity; hence we obtain (setting $f^*_{12\ldots}$ to be the least common multiple of $f^*, f_1, f_2, \ldots$)

$$\prod_{(u^*;u_1,u_2,\ldots)}\left\{1-\left[\frac{p}{\overbrace{u,u^*;u_1,u_2,\ldots}}\right]p^{-s}\right\}=$$

$$\left\{1-\left[\frac{p}{2^2}\right]^{uf^*_{12\ldots}}p^{-sf^*_{12\ldots}}\right\}^{e^*e_1e_2\cdots f_1f_2\cdots/f^*_{12\ldots}}$$

where now the product is taken additionally over all the values of u^* in (26.1).

Finally, let $\bar{e}$ be the greatest common divisor of $\frac{1}{2}(p-1)$ and 2 and set $\bar{f} = 2/\bar{e}$. If F is the least common multiple of the numbers $\bar{f}$, f^*, f_1, f_2, ... and we write

$$E=\frac{\bar{e}e^*e_1e_2\cdots\bar{f}f^*f_1f_2\cdots}{F}$$

then we deduce from the last formula that

$$\prod_{(u,u^*;u_1,u_2,\ldots)}\left\{1-\left[\frac{p}{\overbrace{u,u^*;u_1,u_2,\ldots}}\right]p^{-s}\right\}=\left\{1-p^{-sF}\right\}^E \tag{26.2}$$

where the product is taken over all values of u, u^*, u_1, u_2, ... given in (26.1). We see at once that F is the least positive exponent with the property that $p^F \equiv 1 \pmod{m}$; and in addition $FE = \Phi(m)$. Hence, when we make use of Theorem 125 we deduce from (26.2) the formula asserted in Lemma 22. With the help of the second assertion in Theorem 125 we deduce easily that the formula holds also in the case where p is a prime divisor of m.

The first expression for H in Theorem 141 now follows at once from Theorem 56 if we use the second representation of $\zeta(s)$ in Sect. 27 and apply Lemma 22 which we have just proved.

To derive the second expression for H we transform the infinite product appearing after the limit sign in the first expression into an infinite sum, as follows:

$$\prod_{(p)} \frac{1}{1-\left[\overbrace{u,u^*;u_1,u_2,\ldots}^{p}\right]p^{-s}} = \sum_{(n)} \left[\overbrace{u,u^*;u_1,u_2,\ldots}^{n}\right]\frac{1}{n^s}$$

where the sum on the right hand side is taken over all positive integers n. Further manipulation of the sum is most easily carried out if we make the substitution

$$\frac{1}{n^s} = \frac{1}{\Gamma(s)}\int_0^\infty e^{-nt}t^{s-1}dt$$

and then proceed in the same way as in Sect. 86.

§119. The Existence of Infinitely Many Rational Primes with a Prescribed Residue Modulo a Given Number

Each of the two expressions for the class number H of the cyclotomic field of the m-th roots of unity which we stated in Sect. 117 and have just proved has an important consequence. The first expression serves to prove the following result.

Theorem 143. *Let m and n be relatively prime rational integers. Then there are infinitely many prime numbers p such that $p \equiv n \pmod m$* (*Dirichlet* (5, 6), *Dedekind* (1)).

Proof. Here again we consider the most complicated case, in which m is divisible by 8. As in Sect. 117 we set $m = 2^{h^*}l_1^{h_1}l_2^{h_2}\ldots$ Each of the infinite products

$$\prod_{(p)} \frac{1}{1-\left[\overbrace{u,u^*;u_1,u_2,\ldots}^{p}\right]p^{-s}}$$

occurring there, with the exception of the one corresponding to the values $u = u^* = u_1 = u_2 = \ldots = 0$, converges for $s = 1$ to a determinate limit; from the first expression for the class number H given in Sect. 117 these limits must all be nonzero. Thus we may take the logarithms of these products and then simple calculations similar to those in Sect. 80 lead to the result that for every set of values for u, u^*; u_1, u_2, ... (always excluding the case $u = u^* = u_1 = u_2 = \ldots = 0$) the infinite sum

$$\sum_{(p)} \Big[\underbrace{\qquad p \qquad}_{u, u^*; u_1, u_2, \ldots} \Big] \frac{1}{p^s} \tag{26.3}$$

(where p runs over all rational prime numbers) has a finite limit at $s = 1$.

Since n is supposed relatively prime to m the symbols

$$\left[\frac{n}{2^2}\right], \left[\frac{n}{2^h}\right], \left[\frac{n}{l_1^{h_1}}\right], \left[\frac{n}{l_2^{h_2}}\right], \ldots$$

are all nonzero. We multiply the expression (26.3) by

$$\frac{1}{\left[\frac{n}{2^2}\right]^u \left[\frac{n}{2^h}\right]^{u^*} \left[\frac{n}{l_1^{h_1}}\right]^{u_1} \left[\frac{n}{l_2^{h_2}}\right]^{u_2} \cdots};$$

then, letting $u, u^*; u_1, u_2, \ldots$ run through the values given in (26.1) (with the case $u = u^* = u_1 = u_2 = \ldots = 0$ excluded) and adding all the expressions so formed to the infinite sum (18.1) (see Sect. 80, p. 143) we obtain

$$\left.\begin{aligned} \textstyle\sum_{(p)}(1+P) \quad & (1 + P^* + (P^*)^2 + \cdots + (P^*)^{2^{h^*-2}-1}) \cdot \\ & \cdot (1 + P_1 + (P_1)^2 + \cdots + (P_1)^{l_1^{h_1-1}(l_1-1)-1}) \cdot \\ & \cdot (1 + P_2 + (P_2)^2 + \cdots + (P_2)^{l_2^{h_2-1}(l_2-1)-1}) \cdot \cdots \cdot p^{-s} \end{aligned}\right\} \tag{26.4}$$

where we write

$$P = \frac{\left[\frac{p}{2^2}\right]}{\left[\frac{n}{2^2}\right]}, P^* = \frac{\left[\frac{p}{2^{h^*}}\right]}{\left[\frac{n}{2^{h^*}}\right]}, P_1 = \frac{\left[\frac{p}{l_1^{h_1}}\right]}{\left[\frac{n}{l_1^{h_1}}\right]}, P_2 = \frac{\left[\frac{p}{l_2^{h_2}}\right]}{\left[\frac{n}{l_2^{h_2}}\right]}, \ldots$$

If we omit from the infinite series (26.4) the terms corresponding to the prime divisors $2, l_1, l_2, \ldots$ of m (of which there are only finitely many) the remaining terms of the series sum to $\Phi(m) \sum p^{-s}$ where p runs over only those rational primes for which the values of P, P^*, P_1, P_2, $\ldots$ are all equal to 1, that is for precisely those prime numbers which satisfy the congruence condition in Theorem 143.

Since the infinite sum (18.1) (see p. 143) increases beyond all bounds for $s = 1$, while on the other hand the infinite sums (26.3) all remain finite for $s = 1$, it follows that the value of the infinite sum (26.4) must increase beyond all bounds for $s = 1$. Hence there must necessarily be infinitely many prime numbers satisfying the condition of Theorem 143.

§120. Representation of All the Units of the Cyclotomic Field by Cyclotomic Units

The second of the two expressions given in Sect. 117 enables us to prove the following theorem.

Theorem 144. *Every unit of an abelian field is a root with rational integer exponent of a product of cyclotomic units.*

Proof. Consider first the case where $m = l$ is an odd prime. According to the formula in Theorem 142 the second factor of the class number contains in its numerator a certain determinant Δ. This determinant Δ is thus nonzero. From this it follows, when we take into consideration the results of Sect. 20 and 21, that the $\frac{1}{2}(l-3)$ units $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\frac{1}{2}(l-3)}$ given in Theorem 142 form an independent set of units. This fact establishes the result of Theorem 144 for the particular case of the cyclotomic field $k(e^{2\pi i/l})$ and so also for all its subfields (*Kummer* (11)).

A transformation of the second factor of the class number similar to that given in Theorem 142 is also possible in the case of the cyclotomic field $k(e^{2\pi i/m})$ of the m-th roots of unity where m is an arbitrary composite number; the corresponding expression together with Theorem 131 leads to a proof of the general case of Theorem 144.

A rich store of numerical experimental data of great use for the deeper investigation of the theory of cyclotomic fields is available in the tables of complex prime numbers calculated by Reuschle (*Reuschle* (1), *Kummer* (24), *Kronecker* (12)).

27. Applications of the Theory of Cyclotomic Fields to Quadratic Fields

§121. Generation of the Units of Real Quadratic Fields by Cyclotomic Units

If we apply to a quadratic subfield of the cyclotomic field of the m-th roots of unity some of the properties derived in the preceding chapters then we obtain new theorems about quadratic fields. We render this method even more fruitful by using it in conjunction with the results which we found in Part 3 by direct consideration of quadratic fields.

According to the general Theorem 144 it follows in particular that every unit of a real quadratic field $k(\sqrt{m})$ is a root of a product of cyclotomic units with a rational integer exponent. A special unit of $k(\sqrt{m})$ is given by the following expression

$$\frac{\prod\limits_{(b)}(e^{\pi ib/d} - e^{-\pi ib/d})}{\prod\limits_{(a)}(e^{\pi ia/d} - e^{-\pi ia/d})}$$

where d is the discriminant of the field $k(\sqrt{m})$ and the products $\prod\limits_{(a)}$ and $\prod\limits_{(b)}$ are taken over all the integers a or b in the range $1, 2, \ldots, |d|$ such that $\left(\frac{d}{a}\right) = +1$ or $\left(\frac{d}{b}\right) = -+1$ respectively (*Dirichlet* (7)). Cf Sect. 86.

§122. The Quadratic Reciprocity Law

Let l be an odd prime number, r a primitive root modulo l; let $\zeta = e^{2\pi i/l}$ and $s = (\zeta : \zeta^r)$. The subfield of $k(\zeta)$ belonging to the subgroup of its group consisting of the automorphisms $1, s^2, s^4, \ldots, s^{l-3}$ is a quadratic field k^*. Since, according to Theorem 118, the discriminant of $k(\zeta)$ is $(-1)^{\frac{1}{2}(l-1)}l^{l-2}$, it follows from Theorem 39 that the discriminant of k^* has no rational prime factor other than l and so, by Theorem 95, it has the value $d = (-1)^{\frac{1}{2}(l-1)}l$.

Let p be either the prime number 2 or an arbitrary odd prime number distinct from l. If we carry out the factorisation of p first in the cyclotomic field of the l-th roots of unity and then directly by Theorem 97 in the quadratic subfield k^* and compare the results, we obtain a new proof of the quadratic reciprocity law (*Kronecker* (15)). We proceed as follows.

Let f be the least positive exponent such that $p^f \equiv 1 \pmod{l}$; set $e = (l-1)/f$. Then, according to Theorem 119, the prime number p splits in the field $k(\zeta)$ as a product of e prime ideals $\mathfrak{P}$, $s\mathfrak{P}$, ..., $s^{e-1}\mathfrak{P}$ and, according to Theorem 129, the common decomposition field k_z of these prime ideals is of degree e. The rational prime p then clearly splits or remains prime in k^* according as k^* is a subfield of k_z or not. When we recall that the field $k(\zeta)$ has only the one quadratic subfield k^* and that an abelian field actually has a quadratic subfield if and only if its degree is even, then we see that k^* is included in k_z if and only if the number e is even. On the other hand, according to Theorem 97, the prime number p splits or remains prime in k^* according as $\left(\frac{(-1)^{\frac{1}{2}(l-1)}l}{p}\right) = +1$ or -1. If e is even it follows that $p^{\frac{1}{2}(l-1)} = p^{\frac{1}{2}e\cdot f} \equiv 1 \pmod{l}$, i.e. $\left(\frac{p}{l}\right) = +1$; in the other case we have $p^{\frac{1}{2}(l-1)} = p^{\frac{1}{2}f\cdot e} \equiv (-1)^e \equiv -1 \pmod{l}$, i.e. $\left(\frac{p}{l}\right) = -1$. Thus in each case we have

$$\left(\frac{p}{l}\right) = \left(\frac{(-1)^{\frac{1}{2}(l-1)}l}{p}\right). \tag{27.1}$$

We suppose first that p is odd; from (27.1) it follows that

$$\left(\frac{p}{l}\right)\left(\frac{l}{p}\right) = \left(\frac{(-1)^{\frac{1}{2}(l-1)}}{p}\right) \tag{27.2}$$

and further, if we interchange p and l we obtain

$$\left(\frac{(-1)^{\frac{1}{2}(l-1)}}{p}\right) = \left(\frac{(-1)^{\frac{1}{2}(p-1)}}{l}\right).$$

If we set $l = 3$ this gives

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}. \tag{27.3}$$

Combining (27.3) with (27.2) we obtain

$$\left(\frac{l}{p}\right)\left(\frac{p}{l}\right) = (-1)^{\frac{1}{2}(l-1)\cdot\frac{1}{2}(p-1)}. \tag{27.4}$$

If we set $p = 2$ in (27.1) we have

$$\left(\frac{2}{l}\right) = \left(\frac{(-1)^{\frac{1}{2}(l-1)}l}{2}\right) = (-1)^{\frac{1}{8}(l^2-1)}. \tag{27.5}$$

Equations (27.4), (27.3) and (27.5) are the quadratic reciprocity law and its two supplementary laws.

§123. Imaginary Quadratic Fields with Prime Discriminant

Theorem 145. *Let l be a rational prime number such that $l \equiv 3 \pmod 4$; let p be a rational prime number of the form $p = ml + 1$. Then for each prime ideal $\mathfrak{p}$ of the imaginary quadratic field $k(\sqrt{-l})$ which divides p we have*

$$\mathfrak{p}^{(\sum b - \sum a)/l} \sim 1$$

where $\sum a$ is the sum of the smallest positive quadratic residues and $\sum b$ is the sum of the smallest positive quadratic nonresidues modulo l.

If $p = \mathfrak{p}\mathfrak{p}'$ and

$$\mathfrak{p}^{(\sum b - \sum a)/l} = (\pi)$$

where π is an integer of the imaginary quadratic field $k(\sqrt{-l})$ then we have

$$\pi \equiv \pm \frac{1}{\prod_{(a)}(am)!} \pmod{\mathfrak{p}'},$$

where the product in the denominator is taken over the smallest quadratic residues a modulo l (Jacobi (1, 2, 3, 4), *Cauchy* (1), *Eisenstein* (4)).

Proof. If $\mathfrak{P}$ is a prime ideal of degree 1 in $k(\zeta)$, then, with the notation described in Theorem 136, we have

$$\mathfrak{P}^{q_0 + q_{-1}s + q_{-2}s^2 + \cdots + q_{-l+2}s^{l-2}} = (\mathsf{A}), \tag{27.6}$$

where A is an integer in $k(\zeta)$. If $p = ml + 1$ is the rational prime divisible by $\mathfrak{P}$ and $p = \mathfrak{p}\mathfrak{p}'$ its factorisation in the quadratic subfield $k(\sqrt{-l})$ of $k(\zeta)$ then the prime ideals $\mathfrak{p}$ and $\mathfrak{p}'$ of $k(\sqrt{-l})$ have the form

$$\begin{aligned}\mathfrak{p} &= \mathfrak{P}^{1+s^2+s^4+\cdots+s^{l-3}}\\ \mathfrak{p}' &= s\mathfrak{p} = \mathfrak{P}^{s(1+s^2+s^4+\cdots+s^{l-3})}.\end{aligned}$$

If we raise equation (27.6) to the $(1 + s^2 + s^4 + \cdots + s^{l-3})$-th symbolic power it follows that

$$\mathfrak{p}^{q_0+q_{-2}+q_{-4}+\cdots+q_{-l+3}}(\mathfrak{p}')^{q_{-1}+q_{-3}+q_{-5}+\cdots+q_{-l+2}} = (\alpha),$$

where α is a number in $k(\sqrt{-l})$. Since

$$q_{-1} + q_{-3} + \cdots + q_{-l+2} - q_0 - q_{-2} - \cdots - q_{-l+3} = (r+1)\frac{\sum b - \sum a}{l}$$

it follows, when we take account of the equivalence $\mathfrak{p}\mathfrak{p}' \sim 1$, that

$$\mathfrak{p}^{(r+1)(\sum b - \sum a)/l} \sim 1. \tag{27.7}$$

On the other hand we have, according to Theorem 135,

$$\mathfrak{P}^{r_0+r_{-1}s+r_{-2}s^2+\cdots+r_{-l+2}s^{l-2}} = (\mathsf{B})$$

where B is an integer in $k(\zeta)$. If we now raise this equation to the $(1 + s^2 + s^4 + \cdots + s^{l-3})$-th symbolic power it follows that

$$\mathfrak{p}^{(\sum b - \sum a)} = \mathfrak{p}^{l\cdot(\sum b-\sum a)/l} \sim 1. \tag{27.8}$$

Since the number $r+1$ is not divisible by l (when we disregard the case where $l = 3$ in which the result is immediately clear) the equivalence asserted in the first part of Theorem 145 follows from the equivalences (27.7) and (27.8),

The second part of Theorem 145 follows by a more detailed examination of the congruence properties (24.4) and (24.5) of the Lagrange root number Λ which we developed in Sect. 112.

An essentially different proof for the first part of Theorem 145 follows immediately from a remark we made at the end of Sect. 86 concerning the form of the class number of $k(\sqrt{-l})$ in the case where $l \equiv 3 \pmod 4$.

By a noteworthy modification of Jacobi's procedure it is also possible to extend the statement of Theorem 145 to the case where the prime number p is not of the form $ml + 1$ (*Eisenstein* (11), *Stickelberger* (1)).

§124. Determination of the Sign of the Gauss Sum

Let p be an odd rational prime number. Then, according to the definitions of Sect. 111 and their extension in Sect. 112 to the case where $l = 2$, we can determine the Lagrange normal basis and the Lagrange root number for the quadratic field $k\left(\sqrt{(-1)^{\frac{1}{2}(p-1)}p}\right)$. If we set $\mathsf{Z} = e^{2\pi i/p}$ then the Lagrange normal basis for this field consists of the two numbers

$$\lambda_0 = \sum_{(a)} \mathsf{Z}^a, \lambda_1 = \sum_{(b)} \mathsf{Z}^b$$

and the Lagrange root number has the value

$$\Lambda = \lambda_0 - \lambda_1 = \sum_{(a)} \mathsf{Z}^a - \sum_{(b)} \mathsf{Z}^b$$

where a and b run respectively through the quadratic residues and non-residues modulo p among the numbers $1, 2, \ldots, p-1$. The problem discussed at the end of Sect. 112 of determining Λ completely once Λ^l is found reduces

in the present case of a quadratic field to the determination of a certain sign; it is answered by the following theorem.

Theorem 146. *The Lagrange root number Λ of the quadratic field with prime number discriminant $(-1)^{\frac{1}{2}(p-1)}p$ is a positive real or positive purely imaginary number (Gauss (2), Kronecker (4)).*

Proof. Since the Lagrange root number Λ in question here is a number of the quadratic field and, according to Theorem 138, we have

$$|\Lambda| = |\sqrt{p}|,$$

its square has the value $(-1)^{\frac{1}{2}(p-1)}p$. Hence we have

$$\Lambda = \pm\sqrt{(-1)^{\frac{1}{2}(p-1)}p}. \tag{27.9}$$

In place of the ideals denoted by $\mathfrak{p}$ and $\mathfrak{P}$ in Sect. 112 we have to deal in the present case where $l = 2$ with the ideals (p) and $(1 - \mathsf{Z})$ respectively; the congruence (24.4) thus becomes

$$\Lambda \equiv \frac{(-1)^{\frac{1}{2}(p+1)}}{(\frac{1}{2}(p-1))!}(1-\mathsf{Z})^{\frac{1}{2}(p-1)} \pmod{(1-\mathsf{Z})^{\frac{1}{2}(p+1)}},$$

that is

$$\Lambda \equiv (\tfrac{1}{2}(p-1))!(1-\mathsf{Z})^{\frac{1}{2}(p-1)} \pmod{(1-\mathsf{Z})^{\frac{1}{2}(p+1)}}. \tag{27.10}$$

We consider on the other hand the expression

$$\Delta = (\mathsf{Z}^{-1} - \mathsf{Z}^{+1})(\mathsf{Z}^{-2} - \mathsf{Z}^{+2}) \cdots (\mathsf{Z}^{-\frac{1}{2}(p-1)} - \mathsf{Z}^{+\frac{1}{2}(p-1)}).$$

Since this changes only in sign if we replace Z by Z^R (where R is a primitive root modulo p) and since the ideal (Δ) coincides with the ideal $(1-\mathsf{Z})^{\frac{1}{2}(p-1)}$ we must have

$$\Delta = \pm\sqrt{(-1)^{\frac{1}{2}(p-1)}p}.$$

In order to determine the sign here we bear in mind that

$$\mathsf{Z}^{-h} - \mathsf{Z}^{+h} = -2i\sin\frac{2h\pi}{p} \qquad (h = 1, 2, \ldots, \tfrac{1}{2}(p-1))$$

and from this we obtain a value for Δ of the form $(-i)^{\frac{1}{2}(p-1)}P$ where P is a positive real number. From this it follows that

$$\Delta = (-1)^{\frac{1}{8}(p^2-1)}\sqrt{(-1)^{\frac{1}{2}(p-1)}p}, \tag{27.11}$$

where from now on $\sqrt{(-1)^{\frac{1}{2}(p-1)}p}$ shall be taken to be the value of the square root which is either positive or positive purely imaginary.

Finally, the equation

$$\Delta = Z^{-1-2-\cdots-\frac{1}{2}(p-1)}(1-Z^2)(1-Z^4)\cdots(1-Z^{p-1})$$

shows that

$$\begin{aligned} \Delta &\equiv 2\cdot 4\cdot 6\cdot\cdots\cdot(p-1)(1-Z)^{\frac{1}{2}(p-1)} \\ &\equiv 2^{\frac{1}{2}(p-1)}(\tfrac{1}{2}(p-1))!(1-Z)^{\frac{1}{2}(p-1)} \pmod{(1-Z)^{\frac{1}{2}(p+1)}} \end{aligned}$$

and hence it follows from (27.10) that

$$\Delta \equiv 2^{\frac{1}{2}(p-1)}\Lambda \pmod{(1-Z)^{\frac{1}{2}(p+1)}}.$$

Since

$$2^{\frac{1}{2}(p-1)} \equiv \left(\frac{2}{p}\right) \equiv (-1)^{\frac{1}{8}(p^2-1)} \pmod{p}$$

we obtain from (27.11) that

$$\Lambda \equiv \sqrt{(-1)^{\frac{1}{2}(p-1)}p} \pmod{(1-Z)^{\frac{1}{2}(p+1)}}$$

and hence, according to (27.9), that

$$\Lambda = \sqrt{(-1)^{\frac{1}{2}(p-1)}p}.$$

This completes the proof of Theorem 146.

Up to now very little has been published about special abelian fields of degree greater than 2; we mention, however, Eisenstein's article on cubic forms arising from cyclotomy, which can be seen as an introduction to the theory of cubic abelian fields (*Eisenstein* (10)), Bachmann's work on the complex numbers formed by composing two square roots (*Bachmann* (1)) and Weber's investigations into abelian cubic and biquadratic number fields (*Weber* (2, 4)).

Part V

Kummer Number Fields

28. Factorisation of the Numbers of the Cyclotomic Field in a Kummer Field

§125. Definition of Kummer Fields

Let l be an odd rational prime number and $k(\zeta)$ the cyclotomic field generated by $\zeta = e^{2\pi i/l}$. Let μ be an integer of $k(\zeta)$ which is not the l-th power of a number in $k(\zeta)$; then the l-th degree equation

$$x^l - \mu = 0$$

is irreducible over the field $k(\zeta)$. If we choose a fixed root $\mathsf{M} = \sqrt[l]{\mu}$ of this equation then the remaining $l-1$ roots are

$$\zeta\mathsf{M}, \zeta^2\mathsf{M}, \ldots, \zeta^{l-1}\mathsf{M}.$$

The field $k(\mathsf{M}, \zeta)$ generated by M and ζ is called a *Kummer field.* Such a Kummer field $k(\mathsf{M}, \zeta)$ is of degree $l(l-1)$; it includes the cyclotomic field $k(\zeta)$ as a subfield and is an abelian extension of $k(\zeta)$ of relative degree l. By the operation of replacing M by $\zeta\mathsf{M}$ in a number or an ideal of this Kummer field we obtain the relative conjugate number or ideal. We shall denote this operation by prefixing the substitution symbol S.

The following results are easily proved.

Theorem 147. *Let $s = (\zeta : \zeta^r)$, where r is a primitive root modulo l. Then the Kummer field determined by $\mathsf{M} = \sqrt[l]{\mu}$ and ζ is a Galois extension of the field of rational numbers if and only if there occurs among the symbolic powers μ^{s-1}, μ^{s-2}, ..., μ^{s-l+1} the l-th power of some number in $k(\zeta)$.*

In particular the Kummer field $k(\mathsf{M}, \zeta)$ is an abelian field if and only if μ^{s-r} is the l-th power of a number in $k(\zeta)$.

If the Kummer field $k(\mathsf{M}, \zeta)$ is a Galois or, in particular, an abelian field then it is obtained (as we see using the ideas introduced in Sect. 38) by composing the cyclotomic field $k(\zeta)$ and a field of degree l.

§126. The Relative Discriminant of a Kummer Field

Our first task is to determine the relative discriminant of $k(\mathsf{M},\zeta)$ with respect to $k(\zeta)$. We prove the following result.

Lemma 23. *If a prime ideal $\mathfrak{p}$ of the cyclotomic field $k(\zeta)$ is the l-th power of a prime ideal $\mathfrak{P}$ of the Kummer field $k(\mathsf{M},\zeta)$ and A is an integer of $k(\mathsf{M},\zeta)$ divisible by $\mathfrak{P}$ but not by $\mathfrak{P}^2$ then the relative discriminant of A and the relative discriminant of $k(\mathsf{M},\zeta)$ with respect to $k(\zeta)$ are divisible by precisely the same power of $\mathfrak{p}$.*

Proof. It is clear that every integer Ω of the Kummer field $k(\mathsf{M},\zeta)$ can be represented in the form

$$\Omega = \frac{\alpha + \alpha_1\mathsf{A} + \alpha_2\mathsf{A}^2 + \cdots + \alpha_{l-1}\mathsf{A}^{l-1}}{\beta}, \tag{28.1}$$

where α, α_1, α_2, $\ldots$, α_{l-1}, β are integers in $k(\zeta)$. If β is divisible by $\mathfrak{p}$ it follows that the numerator of the fraction on the right hand side must be congruent to 0 modulo $\mathfrak{p}$. Since $\mathsf{A} \equiv 0 \pmod{\mathfrak{P}}$ it follows that $\alpha \equiv 0$ (mod $\mathfrak{P}$) and so, since α lies in $k(\zeta)$ we actually have $\alpha \equiv 0 \pmod{\mathfrak{p}}$. From this last congruence we have

$$\alpha_1\mathsf{A} + \alpha_2\mathsf{A}^2 + \cdots + \alpha_{l-1}\mathsf{A}^{l-1} \equiv 0 \pmod{\mathfrak{p}}.$$

Since $\mathsf{A} \not\equiv 0$, $\mathsf{A}^2 \equiv 0$, $\ldots$, $\mathsf{A}^{l-1} \equiv 0 \pmod{\mathfrak{P}^2}$ it follows that $\alpha_1 \equiv 0 \pmod{\mathfrak{P}}$ and hence $\alpha_1 \equiv 0 \pmod{\mathfrak{p}}$ so that we have

$$\alpha_2\mathsf{A}^2 + \cdots + \alpha_{l-1}\mathsf{A}^{l-1} \equiv 0 \pmod{\mathfrak{p}}.$$

Since $\mathsf{A}^2 \not\equiv 0$, $\mathsf{A}^3 \equiv 0$, $\ldots$, $\mathsf{A}^{l-1} \equiv 0 \pmod{\mathfrak{P}^3}$ we must have $\alpha_2 \equiv 0$ (mod $\mathfrak{P}$) and hence $\alpha_2 \equiv 0 \pmod{\mathfrak{p}}$. Proceeding in this way we see that all the coefficients α, α_1, α_2, $\ldots$, α_{l-1} must be divisible by $\mathfrak{p}$. If now β' is an integer in $k(\zeta)$ which is divisible by $\beta/\mathfrak{p}$ but not by β then the numbers $\alpha\beta'$, $\alpha_1\beta'$, $\ldots$, $\alpha_{l-1}\beta'$ are all divisible by β. We set

$$\alpha' = \frac{\alpha\beta'}{\beta},\ \alpha_1' = \frac{\alpha_1\beta'}{\beta},\ \ldots, \alpha_{l-1}' = \frac{\alpha_{l-1}\beta'}{\beta}$$

and obtain

$$\Omega = \frac{\alpha' + \alpha_1'\mathsf{A} + \alpha_2'\mathsf{A}^2 + \cdots + \alpha_{l-1}'\mathsf{A}^{l-1}}{\beta'}, \tag{28.2}$$

where the exponent of the power of $\mathfrak{p}$ dividing β' is 1 less than that for β. If we apply to (28.2) the procedure we have just used to deduce it from (28.1) and continue in this way we eventually have the result that every integer Ω

of the field $k(\mathsf{M},\zeta)$ can be represented in the form

$$\Omega = \frac{\bar{\alpha} + \bar{\alpha}_1 \mathsf{A} + \bar{\alpha}_2 \mathsf{A}^2 + \cdots + \bar{\alpha}_{l-1} \mathsf{A}^{l-1}}{\bar{\beta}}, \tag{28.3}$$

where $\bar{\alpha}$, $\bar{\alpha_1}$, ..., $\bar{\alpha_{l-1}}$, $\bar{\beta}$ are all integers in $k(\zeta)$ and $\bar{\beta}$ is prime to $\mathfrak{p}$. Now we represent all the $l(l-1)$ numbers of a basis for the Kummer field $k(\mathsf{M},\zeta)$ in the form (28.3) and consider the l-rowed matrix formed from these numbers and their relative conjugates; it is then obvious that the relative discriminant of the Kummer field $k(\mathsf{M},\zeta)$ on multiplication by an integer $\bar{\beta}$ prime to $\mathfrak{p}$ must be divisible by the relative discriminant of the number A.

This completes the proof of Lemma 23.

Theorem 148. *Let $\lambda = 1 - \zeta$, $\mathfrak{l} = (\lambda)$; let $\mathfrak{p}$ be a prime ideal of $k(\zeta)$ distinct from $\mathfrak{l}$. Let μ be a number of $k(\zeta)$ divisible by $\mathfrak{p}^e$ precisely. If e is prime to l then the relative discriminant with respect to $k(\zeta)$ of the Kummer field generated by $\mathsf{M} = \sqrt[l]{\mu}$ and ζ is divisible by $\mathfrak{p}^{l-1}$ precisely. If e is divisible by l then this relative discriminant is prime to $\mathfrak{p}$.*

As far as the prime ideal $\mathfrak{l}$ is concerned we can first exclude the situation in which the number μ is divisible by a power of $\mathfrak{l}$ whose exponent is divisible by l; for in that case we can replace μ by a number μ^* prime to $\mathfrak{l}$ such that $k(\sqrt[l]{\mu^*},\zeta)$ is the same field as $k(\sqrt[l]{\mu},\zeta)$. When this possibility is excluded we have two cases to consider – (1) when μ is divisible exactly by a power of $\mathfrak{l}$ whose exponent is prime to l; (2) when μ is not divisible by $\mathfrak{l}$. In the first case the relative discriminant of $k(\sqrt[l]{\mu},\zeta)$ with respect to $k(\zeta)$ is divisible by $\mathfrak{l}^{l^2-1}$ precisely. In the second case let m be the greatest exponent not exceeding l for which there exists a number α in $k(\zeta)$ such that $\mu \equiv \alpha^l \pmod{\mathfrak{l}^m}$. Then, if $m = l$, the relative discriminant is prime to $\mathfrak{l}$, while if $m < l$ it is divisible by $\mathfrak{l}^{(l-1)(l-m+1)}$ precisely.

Proof. We begin with the first part of Theorem 148. Let π be an integer of $k(\zeta)$ divisible by $\mathfrak{p}$ but not by $\mathfrak{p}^2$ and let ν be an integer of $k(\zeta)$ divisible by $\pi/\mathfrak{p}$ but prime to $\mathfrak{p}$.

If the exponent e of the precise power of $\mathfrak{p}$ dividing μ is not a multiple of l then we can find two positive rational integers a and b such that $1 = ae - bl$. Then $\mu^* = \mu^a \nu^{bl}/\pi^{bl}$ is an integer of $k(\zeta)$ divisible by $\mathfrak{p}$ but not by $\mathfrak{p}^2$ and it turns out that if we set $\mathsf{M}^* = \sqrt[l]{\mu^*}$ then $k(\mathsf{M}^*,\zeta) = k(\mathsf{M},\zeta)$; furthermore, if we denote the ideal common divisor of M^* and $\mathfrak{p}$ in the field $k(\mathsf{M},\zeta)$ by $\mathfrak{P}$, then

$$\mathfrak{P} = S\mathfrak{P}, \quad \mathfrak{p} = \mathfrak{P}^l.$$

The ideal $\mathfrak{P}$ is thus an ambig prime ideal of the Kummer field $k(\mathsf{M},\zeta)$ with respect to the subfield $k(\zeta)$; hence, according to Theorem 93, $\mathfrak{P}$ occurs as a factor of the relative discriminant of $k(\mathsf{M},\zeta)$ with respect to $k(\zeta)$. Since the number M^* is divisible by $\mathfrak{P}$ but not by $\mathfrak{P}^2$ and since the relative discriminant of M^* with respect to $k(\zeta)$ has the value $(-1)^{\frac{1}{2}(l-1)} l^l (\mu^*)^{l-1}$ it follows from

Lemma 23 that the prime ideal $\mathfrak{p}$ occurs in the relative discriminant of the field $k(\mathsf{M},\zeta)$ to precisely the $(l-1)$-st power.

If, on the other hand, the exponent e of the precise power of $\mathfrak{p}$ dividing μ is a multiple of l then $\mu^* = \mu\nu^e/\pi^e$ is an integer of $k(\zeta)$ not divisible by $\mathfrak{p}$. Since the relative discriminant of $\mathsf{M}^* = \sqrt[l]{\mu^*}$ with respect to $k(\zeta)$ has the value $(-1)^{\frac{1}{2}(l-1)}l^l(\mu^*)^{l-1}$ it is prime to $\mathfrak{p}$. It follows that the same holds for the relative discriminant of the field $k(\mathsf{M},\zeta)$ with respect to $k(\zeta)$.

Now we consider the situation relating to the prime ideal $\mathfrak{l}$. If it happens that the exponent e of the exact power of $\mathfrak{l}$ dividing μ is not a multiple of l then we proceed as we did in the first part of the proof when we dealt with the prime $\mathfrak{p}$. Thus we introduce in place of μ a number μ^* which is divisible by $\mathfrak{l}$ but not by $\mathfrak{l}^2$. Since the relative discriminant of the number $\mathsf{M}^* = \sqrt[l]{\mu^*}$ has the value $(-1)^{\frac{1}{2}(l-1)}l^l(\mu^*)^{l-1}$ it follows from Lemma 23 and the defining property of μ^* that the relative discriminant of the field $k(\mathsf{M},\zeta)$ with respect to $k(\zeta)$ is divisible by $\mathfrak{l}^{l^2-1}$ precisely.

Next we have to consider the case in which μ is not divisible by $\mathfrak{l}$. Let m be the exponent defined for this case in the statement of Theorem 148; by the definition we have $m \leq l$.

Suppose first that $m = l$. Then there is a number α in $k(\zeta)$ such that $\mu \equiv \alpha^l \pmod{\mathfrak{l}^l}$; hence $(\mu-\alpha^l)/\lambda^l$ is an integer in $k(\zeta)$ and so the l-th degree equation in x

$$\frac{(\lambda x-\alpha)^l+\mu}{\lambda^l}=0$$

has all its coefficients integers. Since $x=(\alpha-\mathsf{M})/\lambda$ (where we set $\mathsf{M}=\sqrt[l]{\mu}$) is a root of this equation, we see that the number $\Omega=(\alpha-\mathsf{M})/\lambda$ is an integer of the field $k(\mathsf{M},\zeta)$. The relative discriminant of Ω is $\varepsilon\mu^{l-1}$, where ε is a unit, and consequently the relative discriminant of the field $k(\mathsf{M},\zeta)$ with respect to $k(\zeta)$ is prime to $\mathfrak{l}$.

Secondly, suppose that $m<l$, so that μ cannot be congruent to an l-th power modulo $\mathfrak{l}^l$; we set $\mu \equiv \alpha^l + a\lambda^m$ modulo $\mathfrak{l}^{m+1}$ where α is an integer in $k(\zeta)$, m is the exponent described in the statement of the theorem and a is a rational integer not divisible by l. Now we consider the ideal

$$\mathfrak{A}=(\lambda,\alpha-\mathsf{M}).$$

The number $(\alpha-\mathsf{M})/\lambda$ is certainly not an integer since its relative norm with respect to $k(\zeta)$, namely $(\alpha^l-\mu)/\lambda^l$, must be a fraction since $m<l$ and hence the number $\alpha-\mathsf{M}$ is not divisible by $\mathfrak{l}$; thus the ideal $\mathfrak{A}$ is distinct from $\mathfrak{l}$. On the other hand $\mathfrak{A}$ is also distinct from 1 since the relative norm of the number $\alpha-\mathsf{M}$ is divisible by $\mathfrak{l}^m$ according to the congruence

$$N_k(\alpha-\mathsf{M})=\alpha^l-\mu\equiv -a\lambda^m \pmod{\mathfrak{l}^{m+1}}. \tag{28.4}$$

Since $S\mathfrak{A}=\mathfrak{A}$ we have that $\mathfrak{A}$ is an ambig ideal; since it must be a factor of $\mathfrak{l}$ it follows that under the present conditions $\mathfrak{l}$ must belong to the first of the three types of prime ideals in the subfield which were distinguished in

the proof of Theorem 93 in Sect. 57, i.e. we have $\mathfrak{l} = \mathfrak{L}^l$ where $\mathfrak{L}$ is a prime ideal (obviously of degree 1) in the field $k(\mathsf{M}, \zeta)$. From the congruence (28.4) it follows that $\mathfrak{A} = \mathfrak{L}^m$.

Now we determine two positive rational integers a and b such that $1 = am - bl$ and set

$$\Omega = \frac{(\alpha - \mathsf{M})^a}{\lambda^b}.$$

Since $S\mathsf{M} = \zeta\mathsf{M}$ it follows that

$$S\Omega = \frac{(\alpha - \mathsf{M} + \lambda\mathsf{M})^a}{\lambda^b}$$

and we conclude from this expression that $\Omega - S\Omega$ is divisible by precisely the $(l - m + 1)$-th power of $\mathfrak{L}$. Since the same holds for each difference between any two of the relative conjugates of Ω it follows that the relative discriminant of the number Ω with respect to $k(\zeta)$ is divisible by precisely the $(l - m + 1)(l - 1)$-th power of $\mathfrak{l}$. From this it follows, using Lemma 23, since Ω is divisible by only the first power of $\mathfrak{L}$, that the relative discriminant of the field $k(\mathsf{M}, \zeta)$ with respect to $k(\zeta)$ is divisible by the given power of $\mathfrak{l}$.

The relative discriminant of the Kummer field $k(\mathsf{M}, \zeta)$ with respect to the field $k(\zeta)$ is completely determined by Theorem 148; according to Theorem 39 we can deduce from this relative discriminant the discriminant of the Kummer field $k(\mathsf{M}, \zeta)$.

§127. The Symbol $\left\{\frac{\mu}{\mathfrak{w}}\right\}$

To make further progress it is necessary to generalise the symbol $\left\{\frac{\mu}{\mathfrak{w}}\right\}$ introduced in Sect. 113 as follows, so that it makes sense also in the cases where $\mathfrak{w}$ divides μ and where $\mathfrak{w} = \mathfrak{l}$.

Let $\mathfrak{w}$ be an arbitrary prime ideal in $k(\zeta)$ and μ any integer in $k(\zeta)$ which is not the l-th power of an integer in $k(\zeta)$. If the relative discriminant of the Kummer field generated by $\mathsf{M} = \sqrt[l]{\mu}$ and ζ is divisible by $\mathfrak{w}$ then the symbol $\left\{\frac{\mu}{\mathfrak{w}}\right\}$ has the value 0.

If, on the other hand, the relative discriminant of the field $k(\mathsf{M}, \zeta)$ is not divisible by $\mathfrak{w}$ then, according to Theorem 148, we can find a number α of $k(\zeta)$ such that $\mu^* = \alpha^l\mu$ is an integer of $k(\zeta)$ not divisible by $\mathfrak{w}$. (If μ is itself prime to $\mathfrak{w}$ then $\alpha = 1$ already fulfils this condition.) If $\mathfrak{w} \neq \mathfrak{l}$ we define the symbol in question by setting

$$\left\{\frac{\mu}{\mathfrak{w}}\right\} = \left\{\frac{\mu^*}{\mathfrak{w}}\right\}.$$

If $\mathfrak{w} = \mathfrak{l}$ then, since the relative discriminant of $k(\mathsf{M},\zeta)$ is not divisible by $\mathfrak{l}$, we can, according to Theorem 148, choose α in such a way that we have in addition $\mu^* \equiv 1 \pmod{\mathfrak{l}^l}$. In this case we have a congruence of the form

$$\mu^* \equiv 1 + a\lambda^l \pmod{\mathfrak{l}^{l+1}}$$

where a is a certain integer in the range 0, 1, 2, ..., $l-1$. We then define the symbol $\left\{\frac{\mu}{\mathfrak{l}}\right\}$ by the equation

$$\left\{\frac{\mu}{\mathfrak{l}}\right\} = \zeta^a.$$

If μ is the l-th power of an integer in $k(\zeta)$ and $\mathfrak{w}$ is any prime ideal of $k(\zeta)$ then we define $\left\{\frac{\mu}{\mathfrak{w}}\right\} = 1$.

In this way the value of the symbol $\left\{\frac{\mu}{\mathfrak{w}}\right\}$ is uniquely determined for every integer μ and every prime ideal $\mathfrak{w}$ of $k(\zeta)$; the value is in each case either 0 or else a certain l-th root of unity.

Finally let $\mathfrak{a}$ be any ideal of the field $k(\zeta)$; set $\mathfrak{a} = \mathfrak{p}\mathfrak{q}\cdots\mathfrak{w}$ where $\mathfrak{p}$, $\mathfrak{q}$, ..., $\mathfrak{w}$ are prime ideals of $k(\zeta)$. Then, if μ is any integer of $k(\zeta)$, the symbol $\left\{\frac{\mu}{\mathfrak{a}}\right\}$ is defined by the following equation

$$\left\{\frac{\mu}{\mathfrak{a}}\right\} = \left\{\frac{\mu}{\mathfrak{p}}\right\}\left\{\frac{\mu}{\mathfrak{q}}\right\}\cdots\left\{\frac{\mu}{\mathfrak{w}}\right\}.$$

If $\mathfrak{a}$ and $\mathfrak{b}$ are any ideals in $k(\zeta)$ then it is clear that we have

$$\left\{\frac{\mu}{\mathfrak{a}\mathfrak{b}}\right\} = \left\{\frac{\mu}{\mathfrak{a}}\right\}\left\{\frac{\mu}{\mathfrak{b}}\right\}.$$

§128. The Prime Ideals of a Kummer Field

Let μ be an integer of $k(\zeta)$ such that $\mathsf{M} = \sqrt[l]{\mu}$ is not a number in this field. The problem of factorising the prime ideals of $k(\zeta)$ into prime ideals of the Kummer field $k(\mathsf{M},\zeta)$ is resolved by the following theorem.

Theorem 149. *A prime ideal $\mathfrak{p}$ in $k(\zeta)$ is either the l-th power of a prime ideal in the Kummer field $k(\mathsf{M},\zeta)$ determined by $\mathsf{M} = \sqrt[l]{\mu}$ and ζ or the product of l distinct prime ideals or itself a prime ideal according as $\left\{\frac{\mu}{\mathfrak{p}}\right\} = 0$ or 1 or an l-th root of unity distinct from 1.*

Proof. The first part of the theorem relates to the prime ideals which divide the relative discriminant of the Kummer field $k(\mathsf{M},\zeta)$; according to Theorem 93 these are ambig ideals. From this fact or from the proof of Theorem 148 we deduce the result stated for these prime ideals.

If $\mathfrak{p}$ is a prime ideal which does not divide the relative discriminant of $k(\mathsf{M},\zeta)$ let μ^* be an integer not divisible by $\mathfrak{p}$ such that the quotient μ^*/μ is equal to the l-th power of a number in $k(\zeta)$. The field $k(\mathsf{M},\zeta)$ is then generated also by $\mathsf{M}^* = \sqrt[l]{\mu^*}$ and ζ.

We consider first the case where $\mathfrak{p} \neq \mathfrak{l}$. Then, if it happens that $\left\{\dfrac{\mu^*}{\mathfrak{p}}\right\} = 1$, it follows from Theorem 139 that μ^* is congruent to an l-th power modulo $\mathfrak{p}$. We determine (as is clearly possible) an integer α in $k(\zeta)$ such that

$$\mu^* \equiv \alpha^l \pmod{\mathfrak{p}} \quad \text{and} \quad \mu^* \not\equiv \alpha^l \pmod{\mathfrak{p}^2};$$

then we construct the relatively conjugate ideals

$$\begin{aligned} \mathfrak{P} &= (\mathfrak{p},\ \mathsf{M}^* - \alpha), \\ S\mathfrak{P} &= (\mathfrak{p},\ \zeta\mathsf{M}^* - \alpha), \\ &\quad \cdots\cdots\cdots \\ S^{l-1}\mathfrak{P} &= (\mathfrak{p},\ \zeta^{l-1}\mathsf{M}^* - \alpha) \end{aligned}$$

and easily verify the result that

$$\mathfrak{p} = \mathfrak{P} \cdot S\mathfrak{P} \cdot \cdots \cdot S^{l-1}\mathfrak{P}.$$

Since

$$(\mathfrak{P}, S\mathfrak{P}) = (\mathfrak{p}, \mathsf{M}^* - \alpha, \zeta\mathsf{M}^* - \alpha) = 1$$

it follows that $\mathfrak{P}$ and $S\mathfrak{P}$ and consequently all l prime factors $\mathfrak{P}$, $S\mathfrak{P}$, $\ldots$, $S^{l-1}\mathfrak{P}$ of the ideal $\mathfrak{p}$ are distinct from one another. Thus the prime ideal $\mathfrak{p}$ belongs to the second of the three types of prime ideal of the subfield which were enumerated in the proof of Theorem 93: it splits in $k(\mathsf{M},\zeta)$ as the product of l distinct prime ideals. Conversely, if a prime ideal $\mathfrak{p}$ of the field $k(\zeta)$, where in this case we may have $\mathfrak{p} = \mathfrak{l}$, splits in the field $k(\mathsf{M},\zeta)$ as a product of l distinct prime ideals $\mathfrak{P}$, $S\mathfrak{P}$, $\ldots$, $S^{l-1}\mathfrak{P}$ of $k(\mathsf{M},\zeta)$ then if p is the rational prime number divisible by $\mathfrak{p}$ and $N(\mathfrak{P}) = p^f$ is the norm of $\mathfrak{P}$ we have

$$N(\mathfrak{p}) = N(\mathfrak{P})N(S\mathfrak{P})\cdots N(S^{l-1}\mathfrak{P}) = p^{lf}$$

and hence the norm $n(\mathfrak{p})$ of $\mathfrak{p}$ in the field $k(\zeta)$ is also equal to p^f. The fact that the norms $N(\mathfrak{P})$ and $n(\mathfrak{p})$ are equal allows us to deduce, as in Sect. 57, that every integer of the field $k(\mathsf{M},\zeta)$ is congruent modulo $\mathfrak{P}$ to an integer of the subfield $k(\zeta)$. In particular, if we set $\mathsf{M}^* \equiv \alpha \pmod{\mathfrak{P}}$ where α lies in $k(\zeta)$, it follows that $(\mathsf{M}^*)^l = \mu^* \equiv \alpha^l \pmod{\mathfrak{P}}$; since $\mu^* - \alpha^l$ is in $k(\zeta)$ we must have μ^* congruent to α^l modulo $\mathfrak{p}$ also. Hence $\left\{\dfrac{\mu^*}{\mathfrak{p}}\right\} = \left\{\dfrac{\mu}{\mathfrak{p}}\right\} = 1$. This completes the proof of the last part of Theorem 149 for a prime ideal $\mathfrak{p}$ distinct from $\mathfrak{l}$.

Finally we consider the case of the prime ideal $\mathfrak{l}$. If the relative discriminant of $k(\mathsf{M},\zeta)$ with respect to $k(\zeta)$ is not divisible by $\mathfrak{l}$ then, according to Theorem 148, the number μ^* satisfies a congruence of the form

$$\mu^* \equiv \alpha^l + a\lambda^l \pmod{\mathfrak{l}^{l+1}},$$

where a is a rational integer. If now $\left\{\frac{\mu}{\mathfrak{l}}\right\} = 1$, i.e. if a is divisible by l, we deduce a congruence of the form

$$\mu^* \equiv \alpha^l + a^*\lambda^{l+1} \pmod{\mathfrak{l}^{l+2}},$$

where a^* is also a rational integer. If a^* is not divisible by l we set $\mu^{**} = \mu^*$; if, on the other hand, a^* is divisible by l we set $\mu^{**} = (1+\lambda)^l\mu^* = (1-\lambda^2)^l\mu^*$, from which it follows that

$$\mu^{**} \equiv \alpha^l + \lambda^{l+1}\alpha^l \pmod{\mathfrak{l}^{l+2}}.$$

Thus in both cases the number μ^{**} satisfies a congruence

$$\mu^{**} \equiv \alpha^l + a^{**}\lambda^{l+1} \pmod{\mathfrak{l}^{l+2}},$$

where a^{**} is a rational integer not divisible by l. If we set $\mathsf{M}^{**} = \sqrt[l]{\mu^{**}}$ and

$$\mathfrak{L} = (\lambda, (\alpha - \mathsf{M}^{**})/\lambda)$$

then we obtain the factorisation

$$\mathfrak{l} = \mathfrak{L} \cdot S\mathfrak{L} \cdot \dots \cdot S^{l-1}\mathfrak{L}.$$

Since

$$(\lambda, (\alpha - \mathsf{M}^{**})/\lambda, (\alpha - \zeta\mathsf{M}^{**})/\lambda) = 1$$

it follows that $\mathfrak{L} \neq S\mathfrak{L}$ and hence the l prime ideals $\mathfrak{L}, S\mathfrak{L}, \dots, S^{l-1}\mathfrak{L}$ are all distinct.

Conversely, suppose that $\mathfrak{l}$ has a factorisation of this form in the Kummer field $k(\mathsf{M},\zeta)$; then, according to a remark made earlier which, as we noted at the time, applies also when $\mathfrak{p} = \mathfrak{l}$, the norms of $\mathfrak{L}$ in $k(\mathsf{M},\zeta)$ and of $\mathfrak{l}$ in $k(\zeta)$ coincide. Hence each integer of the field $k(\mathsf{M},\zeta)$ must be congruent modulo $\mathfrak{L}$ to an integer of $k(\zeta)$. Then, since according to Theorem 93 $\mathfrak{l}$ is not a factor of the relative discriminant of $k(\mathsf{M},\zeta)$ with respect to $k(\zeta)$, Theorem 148 allows us to write $\mu^* \equiv \alpha^l \pmod{\mathfrak{l}^l}$ and consequently $(\alpha - \mathsf{M}^*)/\lambda$ is an integer. Since $\mathfrak{L}$ is a prime ideal of degree 1 in $k(\mathsf{M},\zeta)$ this integer is congruent modulo $\mathfrak{L}$ to a rational integer a. Then, if N_k denotes the relative norm with respect to $k(\zeta)$, we have the congruence

$$N_k\Big(\frac{\alpha - \mathsf{M}^*}{\lambda} - a\Big) \equiv 0 \pmod{\mathfrak{l}},$$

i.e.

$$(\alpha - a\lambda)^l - \mu^* \equiv 0 \pmod{\mathfrak{l}^{l+1}};$$

hence $\left\{\frac{\mu^*}{\mathfrak{l}}\right\} = \left\{\frac{\mu}{\mathfrak{l}}\right\} = 1$. These facts establish the last part of Theorem 149 for the prime ideal $\mathfrak{l}$.

By means of Theorem 149 we have obtained, in the present case of the fields $k(\mathsf{M},\zeta)$ and $k(\zeta)$, a simple means of distinguishing the three types of prime ideals of a field with respect to a cyclic extension field of prime degree which we enumerated in Theorem 93.

29. Norm Residues and Non-residues of a Kummer Field

§129. Definition of Norm Residues and Non-residues

As in Sect. 125 let μ be a number in the field $k(\zeta)$ such that $\mathsf{M} = \sqrt[l]{\mu}$ does not lie in $k(\zeta)$ and let $k(\mathsf{M}, \zeta)$ be the Kummer field generated by M and ζ; for each number A in $k(\mathsf{M}, \zeta)$ we shall denote its relative norm with respect to $k(\zeta)$ by $N_k(\mathsf{A})$. Let $\mathfrak{w}$ be a prime ideal of $k(\zeta)$ and ν an integer of $k(\zeta)$. If ν is congruent modulo $\mathfrak{w}$ to the relative norm of an integer of $k(\mathsf{M}, \zeta)$ and if, further, for every higher power $\mathfrak{w}^e$ of $\mathfrak{w}$ there exists an integer A of $k(\mathsf{M}, \zeta)$ such that $\nu \equiv N_k(\mathsf{A}) \pmod{\mathfrak{w}^e}$ then we say that ν is a *norm residue* of $k(\mathsf{M}, \zeta)$ modulo $\mathfrak{w}$. In all other cases we say that ν is a *norm non-residue* of $k(\mathsf{M}, \zeta)$ modulo $\mathfrak{w}$.

§130. Theorem on the Number of Norm Residues. Ramification Ideals

We have the following important theorem.

Theorem 150. *If $\mathfrak{w}$ is a prime ideal of the cyclotomic field $k(\zeta)$ which does not divide the relative discriminant of the Kummer field $k(\mathsf{M}, \zeta)$ then every number ν in $k(\zeta)$ which is prime to $\mathfrak{w}$ is a norm residue of $k(\mathsf{M}, \zeta)$ with respect to $\mathfrak{w}$.*

Suppose on the other hand that $\mathfrak{w}$ is a prime ideal of $k(\zeta)$ which does divide the relative discriminant of $k(\mathsf{M}, \zeta)$. If $\mathfrak{w} \neq \mathfrak{l}$ let e be any positive exponent; if $\mathfrak{w} = \mathfrak{l}$ let e be any positive exponent greater than l. Then of all numbers of $k(\zeta)$ which are prime to $\mathfrak{w}$ and mutually incongruent modulo $\mathfrak{w}^e$ precisely one l-th are norm residues modulo $\mathfrak{w}$.

Proof. First let $\mathfrak{w}$ be a prime ideal distinct from $\mathfrak{l}$ in the cyclotomic field $k(\zeta)$ which does not divide the relative discriminant of $k(\mathsf{M}, \zeta)$. There are then two cases to be distinguished, according as $\mathfrak{w}$ splits in $k(\mathsf{M}, \zeta)$ or not. In the first case let $\mathfrak{W}$ be a prime ideal of the Kummer field $k(\mathsf{M}, \zeta)$ which divides $\mathfrak{w}$.

Referring to the proof of Theorem 148 we see that we may suppose without loss of generality that the number μ, and hence also the relative discriminant of the number $\mathsf{M} = \sqrt[l]{\mu}$ with respect to $k(\zeta)$, are not divisible by $\mathfrak{W}$. There are then l integers $\mathsf{A}_1, \mathsf{A}_2, \ldots, \mathsf{A}_l$ satisfying the l congruences

$$\left.\begin{array}{lllllll} \mathsf{A}_1 & + \mathsf{A}_2\mathsf{M} & + & \cdots & + \mathsf{A}_l\mathsf{M}^{l-1} & \equiv & \nu \\ \mathsf{A}_1 & + \mathsf{A}_2\zeta\mathsf{M} & + & \cdots & + \mathsf{A}_l(\zeta\mathsf{M})^{l-1} & \equiv & 1 \\ \mathsf{A}_1 & + \mathsf{A}_2\zeta^2\mathsf{M} & + & \cdots & + \mathsf{A}_l(\zeta^2\mathsf{M})^{l-1} & \equiv & 1 \\ & & & \cdots\cdots & & & \\ \mathsf{A}_1 & + \mathsf{A}_2\zeta^{l-1}\mathsf{M} & + & \cdots & + \mathsf{A}_l(\zeta^{l-1}\mathsf{M})^{l-1} & \equiv & 1 \end{array}\right\} \pmod{\mathfrak{W}}.$$

Now obviously each integer of the field $k(\mathsf{M}, \zeta)$ is congruent modulo $\mathfrak{W}$ to an integer of $k(\zeta)$; we set

$$\mathsf{A}_1 \equiv \alpha_1, \quad \mathsf{A}_2 \equiv \alpha_2, \quad \ldots, \quad \mathsf{A}_l \equiv \alpha_l \pmod{\mathfrak{W}},$$

where $\alpha_1, \alpha_2, \ldots, \alpha_l$ are integers of $k(\zeta)$ and

$$\mathsf{A} = \alpha_1 + \alpha_2\mathsf{M} + \cdots + \alpha_l\mathsf{M}^{l-1}.$$

From this we have

$$\nu \equiv \mathsf{A}, \quad 1 \equiv S\mathsf{A}, \quad \ldots, \quad 1 \equiv S^{l-1}\mathsf{A} \pmod{\mathfrak{W}}$$

and on multiplying these congruences we have that ν is congruent to $N_k(\mathsf{A})$ modulo $\mathfrak{W}$ and hence modulo $\mathfrak{w}$. Thus under the conditions at present applied to the prime ideal $\mathfrak{w}$ we have established the first part of the theorem for the case where $e = 1$. To deal with the case where $e > 1$ we suppose that $\nu \not\equiv N_k(\mathsf{A}) \pmod{\mathfrak{w}^2}$ and set

$$\frac{\nu}{N_k(\mathsf{A})} \equiv 1 + \omega \pmod{\mathfrak{w}^2}$$

where ω is an integer in $k(\zeta)$ which is divisible by $\mathfrak{w}$ but not by $\mathfrak{w}^2$. Let l^* be a rational integer such that $ll^* \equiv 1 \pmod{\mathfrak{w}}$; then we have $\nu \equiv N_k(\mathsf{B}) \pmod{\mathfrak{w}^2}$ where B is the integer $\mathsf{A}(1 + l^*\omega)$. By an appropriate repetition of the procedure adopted here we obtain eventually an integer of $k(\mathsf{M}, \zeta)$ whose relative norm with respect to $k(\zeta)$ is congruent to ν modulo an arbitrarily high power $\mathfrak{w}^e$ of $\mathfrak{w}$.

On the other hand, suppose that $\mathfrak{w}$ does not split in the field $k(\mathsf{M}, \zeta)$; here we can again arrange that μ is not divisible by $\mathfrak{w}$ and hence, by Theorem 149, not an l-th power residue modulo $\mathfrak{w}$. Let $r = (n(\mathfrak{w}) - 1)/l$; then according to the discussion following Theorem 139 there are precisely r l-th power residues in $k(\zeta)$ prime to $\mathfrak{w}$; let these be denoted by $\rho_1, \ldots, \rho_r$. Then the $n(\mathfrak{w}) - 1$ numbers

$$\rho_i\mu^g \quad (i = 1, 2, \ldots, r; g = 0, 1, 2, \ldots, l-1)$$

are all incongruent to one another modulo $\mathfrak{w}$ since μ is not an l-th power residue modulo $\mathfrak{w}$; hence every number in $k(\zeta)$ prime to $\mathfrak{w}$ is congruent

modulo $\mathfrak{w}$ to one of these numbers. If we set $\rho_1 \equiv \alpha_1^l, \ldots, \rho_r \equiv \alpha_r^l$, where $\alpha_1, \ldots, \alpha_r$ are numbers in $k(\zeta)$, it follows that

$$\rho_i \mu^g \equiv N_k(\alpha_i \mathsf{M}^g) \pmod{\mathfrak{w}}$$

and hence every number in $k(\zeta)$ prime to $\mathfrak{w}$ is congruent modulo $\mathfrak{w}$ to the norm of a number in $k(\mathsf{M}, \zeta)$. From this we deduce further, just as in the earlier case, that for every integer ν in $k(\zeta)$ prime to $\mathfrak{w}$ and every power $\mathfrak{w}^e$ of $\mathfrak{w}$ we can find an integer of $k(\mathsf{M}, \zeta)$ whose relative norm is congruent to ν modulo $\mathfrak{w}^e$.

We shall now prove the first part of the theorem for the case where $\mathfrak{w} = \mathfrak{l}$; here we may suppose that μ is prime to $\mathfrak{l}$. We denote by λ^m the highest power of λ which divides $\mu^{l-1} - 1$; of course we have $m \geq 1$. We set

$$\mu^{l-1} \equiv 1 + a\lambda^m \pmod{\mathfrak{l}^{m+1}}$$

where a is a rational integer prime to l. Let a^* be a rational integer such that $aa^* \equiv -1 \pmod{l}$ and set $\mu^* = \mu^{a^*(l-1)}$. Then we have

$$\mu^* \equiv 1 - \lambda^m \pmod{\mathfrak{l}^{m+1}}. \tag{29.1}$$

On the other hand we have the congruences

$$\left.\begin{array}{lcl} (1-\lambda^{g+1})^l & \equiv & 1+\lambda^{l+g} \\ (1-\lambda^{g+1})^{hl} & \equiv & 1+h\lambda^{l+g} \end{array}\right\} \pmod{\mathfrak{l}^{l+g+1}} \tag{29.2}$$

where g is any positive rational integer and h is any positive rational integer prime to l. Since in the case currently under consideration the relative discriminant of $k(\mathsf{M}, \zeta)$ with respect to $k(\zeta)$ is not divisible by $\mathfrak{l}$ it follows from Theorem 148 that we must have $m \geq l$.

Suppose first that $m = l$. Then we conclude easily from the congruences (29.1) and (29.2) that for every positive rational integer g there exists an integer α_g of $k(\zeta)$ such that

$$\mu^* \alpha_g^l \equiv 1 - \lambda^l + \lambda^{l+g} \pmod{\mathfrak{l}^{l+g+1}}.$$

Now we set $\mathsf{M}^* = \sqrt[l]{\mu^*}$ and in general for each value of g we define

$$\Omega_g = \frac{1 - \alpha_g \mathsf{M}^*}{\lambda};$$

then Ω_g is always an integer of $k(\mathsf{M}, \zeta)$ and

$$N_k(\Omega_g) \equiv 1 - \lambda^g \pmod{\mathfrak{l}^{g+1}}.$$

From this it follows immediately that every integer ν in $k(\zeta)$ which satisfies the congruence $\nu \equiv 1 \pmod{\mathfrak{l}}$ is a norm residue of the field $k(\mathsf{M}, \zeta)$ modulo $\mathfrak{l}$. The restriction imposed by the condition that $\nu \equiv 1 \pmod{\mathfrak{l}}$ is easily removed. To see this let ν be any number prime to $\mathfrak{l}$; if it is congruent modulo $\mathfrak{l}$ to the rational integer a we set $\nu^* = (a^*)^l \nu$ where a^* is a rational integer such that

$aa^* \equiv 1 \pmod{\mathfrak{l}}$. Then we have $\nu^* \equiv 1 \pmod{\mathfrak{l}}$ and furthermore ν and ν^* are either both norm residues or both norm non-residues of $k(\mathsf{M}, \zeta)$ modulo $\mathfrak{l}$.

Secondly suppose that in the formula (29.1) we have $m > l$ and hence $\left\{\frac{\mu^*}{l}\right\} = 1$; then if g is any positive rational integer we can always find two integers α_g and α_{g+1} in $k(\zeta)$ such that

$$\left.\begin{aligned} \mu^* \alpha_g^l &\equiv 1 + \lambda^{l+1} + \lambda^{l+g+1} \pmod{\mathfrak{l}^{l+g+2}}, \\ \mu^* \alpha_{g+1}^l &\equiv 1 + \lambda^{l+1} + \lambda^{l+g+2} \pmod{\mathfrak{l}^{l+g+3}}. \end{aligned}\right\} \tag{29.3}$$

According to Theorem 149 we set $\mathfrak{l} = \mathfrak{L} \cdot \mathfrak{L}' \cdot \dots \cdot \mathfrak{L}^{(l-1)}$ where $\mathfrak{L}$, $\mathfrak{L}'$, ..., $\mathfrak{L}^{(l-1)}$ are distinct prime ideals of $k(\mathsf{M}, \zeta)$. The numbers

$$\mathsf{A}_g = \frac{1 - \alpha_g \mathsf{M}^*}{\lambda}, \quad \mathsf{A}_{g+1} = \frac{1 - \alpha_{g+1} \mathsf{M}^*}{\lambda}$$

(where $\mathsf{M}^* = \sqrt[l]{\mu^*}$) are integers and since $N_k(\mathsf{A}_g) \equiv -\lambda \pmod{\mathfrak{l}^2}$ it follows that A_g is divisible by one of the prime ideal factors of $\mathfrak{l}$, say $\mathfrak{L}$, raised to the first power, but by none of the others. From the formulæ (29.3) it follows that

$$\alpha_g^l \equiv \alpha_{g+1}^l \pmod{\mathfrak{l}^{l+2}},$$

and we can now suppose that α_{g+1} is chosen from the numbers α_{g+1}, $\zeta\alpha_{g+1}$, ..., $\zeta^{l-1}\alpha_{g+1}$ in such a way that $\alpha_g \equiv \alpha_{g+1} \pmod{\mathfrak{l}^2}$ and thus $\mathsf{A}_g \equiv \mathsf{A}_{g+1} \pmod{\mathfrak{l}}$. From this last congruence it follows that A_{g+1} is also divisible by $\mathfrak{L}$ but by none of the other prime ideals $\mathfrak{L}'$, ..., $\mathfrak{L}^{(l-1)}$; and since we also have $N_k(\mathsf{A}_{g+1}) \equiv -\lambda \pmod{\mathfrak{l}^2}$ we see that A_{g+1} is divisible by only the first power of $\mathfrak{L}$. From what we have just proved we see that we can write the number $\mathsf{A}_g/\mathsf{A}_{g+1}$ as a fraction whose numerator and denominator are both prime to $\mathfrak{l}$. If we set $\mathsf{A}_g/\mathsf{A}_{g+1} \equiv \Omega_g \pmod{\mathfrak{l}^{g+1}}$ where Ω_g is an integer in $k(\mathsf{M}, \zeta)$, then we have

$$N_k(\Omega_g) \equiv \frac{N_k(\mathsf{A}_g)}{N_k(A_{g+1})} \equiv 1 + \lambda^g \pmod{\mathfrak{l}^{g+1}}.$$

Since we can produce such a formula for each positive exponent g it follows as before that every number prime to $\mathfrak{l}$ is a norm residue of the field $k(\mathsf{M}, \zeta)$.

We now proceed to the proof of the second half of Theorem 150. First let $\mathfrak{w}$ be a prime ideal, distinct from $\mathfrak{l}$, which divides the relative discriminant of the field $k(\mathsf{M}, \zeta)$ with respect to $k(\zeta)$; then, according to Theorem 149, we have $\mathfrak{w} = \mathfrak{W}^l$ where $\mathfrak{W}$ is a prime ideal of $k(\mathsf{M}, \zeta)$. Then, as we have already mentioned several times, each integer of $k(\mathsf{M}, \zeta)$ must be congruent modulo $\mathfrak{W}$ to an integer in $k(\zeta)$. Suppose now that an integer ν of $k(\zeta)$ prime to $\mathfrak{w}$ is congruent modulo $\mathfrak{w}$ to the relative norm $N_k(\mathsf{A})$ of an integer A in $k(\mathsf{M}, \zeta)$; if we have $\mathsf{A} \equiv \alpha \pmod{\mathfrak{W}}$ (where α is an integer of $k(\zeta)$) it follows that ν is congruent to α^l modulo $\mathfrak{W}$ and hence modulo $\mathfrak{w}$, i.e. ν is an l-th power residue modulo $\mathfrak{w}$. Conversely, if a number ν in $k(\zeta)$ is an l-th power residue modulo $\mathfrak{w}$ then ν is obviously also congruent modulo $\mathfrak{w}$ to a relative norm

$N_k(\mathsf{A})$. We deduce from this that the l-th power residues modulo $\mathfrak{w}$ are at the same time all the norm residues of $k(\mathsf{M},\zeta)$ modulo $\mathfrak{w}$.

Finally we have to deal with the case in which $\mathfrak{w} = \mathfrak{l}$ and $\mathfrak{l}$ divides the relative discriminant of $k(\mathsf{M},\zeta)$. In this case we have $\mathfrak{l} = \mathfrak{L}^l$ where $\mathfrak{L}$ is a prime ideal in $k(\mathsf{M},\zeta)$ and in view of Theorem 148 we can arrange that the number μ satisfies either the congruence

$$\mu \equiv \lambda \pmod{\mathfrak{l}^2}$$

or one of the congruences

$$\mu \equiv 1 + \lambda^m \pmod{\mathfrak{l}^{m+1}}$$

where m is one of the integers 1, 2, ..., $l-1$. We shall then investigate in these two cases which numbers of $k(\zeta)$ are congruent to the relative norm of a number in $k(\mathsf{M},\zeta)$ modulo $\mathfrak{l}^{l+1}$ or $\mathfrak{l}^l$ respectively and easily deduce from this the number of mutually incongruent norm residues modulo each higher power of $\mathfrak{l}$.

In the case where $\mu \equiv \lambda \pmod{\mathfrak{l}^2}$ M is divisible by $\mathfrak{L}$ but not by $\mathfrak{L}^2$ and we have the congruences

$$\left.\begin{array}{rcll} N_k(1+\mathsf{M}) & \equiv & 1+\lambda & \pmod{\mathfrak{l}^2} \\ i.e.\ N_k(1+\mathsf{M}) & \equiv & 1+\lambda+\lambda^2\rho_1 & \pmod{\mathfrak{l}^{l+1}} \\ \\ N_k(1+\mathsf{M}^2) & \equiv & 1+\lambda^2 & \pmod{\mathfrak{l}^3} \\ i.e.\ N_k(1+\mathsf{M}^2) & \equiv & 1+\lambda^2+\lambda^3\rho_2 & \pmod{\mathfrak{l}^{l+1}} \\ & & \cdots\cdots\cdots & \\ N_k(1+\mathsf{M}^{l-1}) & \equiv & 1+\lambda^{l-1} & \pmod{\mathfrak{l}^l} \\ i.e.\ N_k(1+\mathsf{M}^{l-1}) & \equiv & 1+\lambda^{l-1}+\lambda^l\rho_{l-1} & \pmod{\mathfrak{l}^{l+1}} \end{array}\right\} \qquad (29.4)$$

where $\rho_1, \rho_2, \ldots, \rho_{l-1}$ are integers of $k(\zeta)$. Finally we have

$$N_k(1+\lambda^t\mathsf{M}^g) \equiv 1 \pmod{\mathfrak{l}^{l+1}} \qquad (29.5)$$

for $t = 1, 2, 3, \ldots$; $g = 0, 1, 2, \ldots, l-1$. Now obviously each integer A of $k(\mathsf{M},\zeta)$ which is prime to $\mathfrak{L}$ satisfies a congruence of the form

$$\begin{array}{rcl} \mathsf{A} & \equiv & a(1+\mathsf{M})^{a_1}(1+\mathsf{M}^2)^{a_2}\cdots(1+\mathsf{M}^{l-1})^{a_{l-1}}\cdot \\ & & \cdot(1+\lambda\mathsf{M})^{a_1'}(1+\lambda\mathsf{M}^2)^{a_2'}\cdots(1+\lambda\mathsf{M}^{l-1})^{a_{l-1}'}\cdot \\ & & \cdots\cdots\cdots \\ & & \cdot(1+\lambda^l\mathsf{M})^{a_1^{(l)}}(1+\lambda^l\mathsf{M}^2)^{a_2^{(l)}}\cdots(1+\lambda^l\mathsf{M}^{l-1})^{a_{l-1}^{(l)}} \pmod{\mathfrak{l}^{l+1}} \end{array}$$

where a is one of the numbers 1, 2, ..., $l-1$ and the $(l+1)(l-1)$ exponents $a_1, a_2, \ldots, a_{l-1}^{(l)}$ are rational integers in the range 0, 1, 2, ..., $l-1$. According to the congruences (29.4) and (29.5) it follows that

$$N_k(\mathsf{A}) \equiv a^l(1+\lambda+\lambda^2\rho_1)^{a_1}(1+\lambda^2+\lambda^3\rho_2)^{a_2}\cdots(1+\lambda^{l-1}+\lambda^l\rho_{l-1})^{a_{l-1}} \pmod{\mathfrak{l}^{l+1}}.$$

When a runs through the values $1, 2, \dots, l-1$ and the exponents $a_1, a_2, \dots, a_{l-1}$ run independently through the range $0, 1, 2, \dots, l-1$ the expression on the right hand side represents $(l-1)l^{l-1}$ numbers and it is easy to see that these are all incongruent to one another modulo $\mathfrak{l}^{l+1}$. Now each number in $k(\zeta)$ which is prime to $\mathfrak{l}$ and congruent modulo $\mathfrak{l}^{l+1}$ to the relative norm $N_k(\mathsf{A})$ of a number in $k(\mathsf{M},\zeta)$ is necessarily congruent modulo $\mathfrak{l}^{l+1}$ to an expression of this form and conversely, as we see from (29.4), each expression of this form is congruent modulo $\mathfrak{l}^{l+1}$ to the relative norm of a number in $k(\mathsf{M},\zeta)$. With the help of the congruences (29.2) we see that any two numbers of $k(\zeta)$ prime to $\mathfrak{l}$ which are congruent to one another modulo $\mathfrak{l}^{l+1}$ are either both norm residues or both norm non-residues modulo $\mathfrak{l}$. The number of norm residues modulo $\mathfrak{l}$ which are prime to $\mathfrak{l}$ and mutually incongruent modulo $\mathfrak{l}^{l+1}$ is thus precisely $(l-1)l^{l-1}$, i.e. one l-th of the total number of numbers in $k(\zeta)$ prime to $\mathfrak{l}$ and mutually incongruent modulo $\mathfrak{l}^{l+1}$; this result can be extended immediately to the powers $\mathfrak{l}^e$ with exponent e greater than $l+1$.

For the sake of brevity we shall consider only the simplest among the remaining possibilities for μ; namely we suppose that $\mu \equiv 1 + \lambda \pmod{\mathfrak{l}^2}$. Set $\Omega = \mathsf{M} - 1$; then Ω is an integer of $k(\mathsf{M},\zeta)$ which is divisible by $\mathfrak{L}$ but not by $\mathfrak{L}^2$. When we recall that $N_k(\Omega) \equiv \lambda \pmod{\mathfrak{l}^2}$ we obtain after some simple calculations the following congruences

$$\left.\begin{array}{rcll} N_k(1+\Omega) & \equiv & 1+\lambda & (\mathrm{mod}\ \mathfrak{l}^2) \\ \text{i.e. } N_k(1+\Omega) & \equiv & 1+\lambda+\lambda^2\rho_1 & (\mathrm{mod}\ \mathfrak{l}^l) \\ & & & \\ N_k(1+\Omega^2) & \equiv & 1+\lambda^2 & (\mathrm{mod}\ \mathfrak{l}^3) \\ \text{i.e. } N_k(1+\Omega^2) & \equiv & 1+\lambda^2+\lambda^3\rho_2 & (\mathrm{mod}\ \mathfrak{l}^l) \\ & & \cdots\cdots\cdots & \\ N_k(1+\Omega^{l-2}) & \equiv & 1+\lambda^{l-2} & (\mathrm{mod}\ \mathfrak{l}^{l-1}) \\ \text{i.e. } N_k(1+\Omega^{l-2}) & \equiv & 1+\lambda^{l-2}+\lambda^{l-1}\rho_{l-1} & (\mathrm{mod}\ \mathfrak{l}^l) \end{array}\right\} \qquad (29.6)$$

where $\rho_1, \rho_2, \dots, \rho_{l-2}$ are certain integers in $k(\zeta)$. Further, we have

$$N_k(1+\Omega^{l-1}) = 1 + \Sigma_1 + \Sigma_2 + \Sigma_3 + \cdots + \Sigma_{l-1} + N_k(\Omega^{l-1})$$

where we write for brevity

$$\begin{array}{rcl} \Sigma_1 & = & \Omega^{l-1} + (S\Omega)^{l-1} + \cdots + (S^{l-1}\Omega)^{l-1}, \\ \Sigma_2 & = & \Omega^{l-1}(S\Omega)^{l-1} + (S\Omega)^{l-1}(S^2\Omega)^{l-1} + \cdots + (S^{l-2}\Omega)^{l-1}(S^{l-1}\Omega)^{l-1}, \\ \Sigma_3 & = & \Omega^{l-1}(S\Omega)^{l-1}(S^2\Omega)^{l-1} + \cdots + (S^{l-3}\Omega)^{l-1}(S^{l-2}\Omega)^{l-1}(S^{l-1}\Omega)^{l-1}, \\ & & \cdots\cdots\cdots \end{array}$$

We have at once that $\Sigma_1 = l$. The individual summands in the expressions for $\Sigma_2, \Sigma_3, \dots, \Sigma_{l-1}$ are all divisible by $\mathfrak{L}^l$; they can be collected into l-element subsets in which all l summands can be obtained from any one of them by applying the automorphisms $1, S, S^2, \dots, S^{l-1}$. If we write an arbitrary term in the form $\lambda\Phi$ then Φ is an integer of $k(\mathsf{M},\zeta)$ and hence, as we see from the

proof of Lemma 23, can be expressed as a polynomial in Ω, and hence as a polynomial in M, whose coefficients are numbers in $k(\zeta)$ all with denominator prime to $\mathfrak{l}$. Accordingly we set $\Phi = F(\mathsf{M})$; then the sum of the corresponding l-element subset can be expressed in the form

$$\lambda\{F(\mathsf{M}) + F(\zeta\mathsf{M}) + F(\zeta^2\mathsf{M}) + \cdots + F(\zeta^{l-1}\mathsf{M})\};$$

it is easily seen that the sum within the braces turns out to be congruent to 0 modulo l; hence the numbers $\Sigma_2, \Sigma_3, \ldots, \Sigma_{l-1}$ are all congruent to 0 modulo $\mathfrak{l}^l$ and so

$$N_k(1 + \Omega^{l-1}) \equiv 1 + l + \lambda^{l-1} \equiv 1 \pmod{\mathfrak{l}^l}. \tag{29.7}$$

Finally we easily obtain the congruences

$$N_k(1 + \lambda^t \Omega^g) \equiv 1 \pmod{\mathfrak{l}^l} \tag{29.8}$$

for $t = 1, 2, 3, \ldots; g = 1, 2, 3, \ldots, l-1$.

Now clearly each integer A of $k(\mathsf{M}, \zeta)$ prime to $\mathfrak{L}$ satisfies a congruence of the form

$$\begin{aligned} \mathsf{A} \equiv\ & a(1+\Omega)^{a_1}(1+\Omega^2)^{a_2}\cdots(1+\Omega^{l-1})^{a_{l-1}}\cdot \\ & \cdot(1+\lambda\Omega)^{a'_1}(1+\lambda\Omega^2)^{a'_2}\cdots(1+\lambda\Omega^{l-1})^{a'_{l-1}}\cdot \\ & \cdots\cdots\cdots \\ & \cdot(1+\lambda^{l-1}\Omega)^{a_1^{(l-1)}}(1+\lambda^{l-1}\Omega^2)^{a_2^{(l-1)}}\cdots(1+\lambda^{l-1}\Omega^{l-1})^{a_{l-1}^{(l-1)}} \pmod{\mathfrak{l}^l}, \end{aligned}$$

where a is one of the numbers $1, 2, \ldots, l-1$ and the $l(l-1)$ exponents $a_1, a_2, \ldots, a_{l-1}^{(l-1)}$ lie in the range $0, 1, 2, \ldots, l-1$. According to the congruences (29.6), (29.7) and (29.8) which we have just established, it follows that

$$N_k(\mathsf{A}) \equiv a^l(1+\lambda+\lambda^2\rho_1)^{a_1}(1+\lambda^2+\lambda^3\rho_2)^{a_2}\cdots(1+\lambda^{l-2}+\lambda^{l-1}\rho_{l-2})^{a_{l-2}} \pmod{\mathfrak{l}^l}.$$

If a runs through the range $1, 2, \ldots, l-1$ and the exponents $a_1, a_2, \ldots, a_{l-2}$ independently of one another run through the range $0, 1, 2, \ldots, l-1$ then the expression on the right hand side represents $(l-1)l^{l-2}$ numbers, all prime to $\mathfrak{l}$ and mutually incongruent modulo $\mathfrak{l}^l$. Using the fact that $N_k(1+\lambda\mathsf{M}) \equiv 1+\lambda^l \pmod{\mathfrak{l}^{l+1}}$ and the congruences (29.2) we conclude that precisely one l-th of all the numbers prime to $\mathfrak{l}$ and incongruent to one another modulo $\mathfrak{l}^l$ are norm residues of the field $k(\mathsf{M}, \zeta)$ modulo $\mathfrak{l}$ and we may extend this result at once to the case of powers $\mathfrak{l}^e$ where $e = l+1$ and $e > l+1$ respectively.

The same result is also obtained, by means of similar calculations, if we suppose that $\mu \equiv 1 \pmod{\mathfrak{l}^2}$ and hence Theorem 150 is completely proved. We should remark, however, that we can organise our later discussion in such a way that Theorem 150 is required only in the case where we have $\mu \equiv 1+\lambda \pmod{\mathfrak{l}^2}$ which we proved in detail above.

Theorem 150 gives expression to a new deep property of the prime ideal factors $\mathfrak{w}$ of the relative discriminant of $k(\mathsf{M},\zeta)$ with respect to $k(\zeta)$. This property corresponds in a certain sense to the well-known theorem concerning the branch points of a Riemann surface according to which an algebraic function in the neighbourhood of a branch point of multiplicity l maps a complete disc conformally onto the l-th part of a disc. In consequence of this I propose to give the name *ramification ideals* for the field $k(\mathsf{M},\zeta)$ to those prime ideals $\mathfrak{w}$ which divide the relative discriminant of $k(\mathsf{M},\zeta)$ with respect to $k(\zeta)$. The terms "ramification ideal" and "prime factor of the relative discriminant" thus have the same meaning; and the ramification ideals are the l-th powers of the ambig prime ideals.

§131. The Symbol $\left\{\dfrac{\nu,\mu}{\mathfrak{w}}\right\}$

Theorem 150 suggests the possibility of classifying the numbers of $k(\zeta)$ which are mutually incongruent modulo a power $\mathfrak{w}^e$ (where $e > l$ in the case $\mathfrak{w} = \mathfrak{l}$) into l subsets, all with the same number of members, one of which consists of the norm residues modulo $\mathfrak{w}$. In order to carry out this classification in a precise way we introduce a new symbol $\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\}$ where ν and μ are nonzero integers of the field $k(\zeta)$ and $\mathfrak{w}$ is a prime ideal of $k(\zeta)$. The value of the symbol is an l-th root of unity, determined as follows.

First let $\mathfrak{w}$ be distinct from $\mathfrak{l}$. In this case if ν is divisible precisely by $\mathfrak{w}^b$ and μ by $\mathfrak{w}^a$ we introduce the number $\kappa = \nu^a/\mu^b$ and reduce it to a fraction ρ/σ where neither the numerator ρ nor the denominator σ is divisible by $\mathfrak{w}$. The symbol $\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\}$ is then defined by the formula

$$\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\} = \left\{\frac{\kappa}{\mathfrak{w}}\right\} = \left\{\frac{\rho}{\mathfrak{w}}\right\}\left\{\frac{\sigma}{\mathfrak{w}}\right\}^{-1}.$$

We deduce at once the following simple rules for these symbols:

$$\left.\begin{aligned} \left\{\frac{\nu_1\nu_2,\mu}{\mathfrak{w}}\right\} &= \left\{\frac{\nu_1,\mu}{\mathfrak{w}}\right\}\left\{\frac{\nu_2,\mu}{\mathfrak{w}}\right\} \\ \left\{\frac{\nu,\mu_1\mu_2}{\mathfrak{w}}\right\} &= \left\{\frac{\nu,\mu_1}{\mathfrak{w}}\right\}\left\{\frac{\nu,\mu_2}{\mathfrak{w}}\right\} \\ \left\{\frac{\nu,\mu}{\mathfrak{w}}\right\}\left\{\frac{\mu,\nu}{\mathfrak{w}}\right\} &= 1 \end{aligned}\right\} \qquad (29.9)$$

where ν, ν_1, ν_2, μ, μ_1, μ_2 are any nonzero integers in $k(\zeta)$.

In order to define the new symbol for the case $\mathfrak{w} = \mathfrak{l}$ we make use of the following considerations.

If ω is any integer in $k(\zeta)$ which satisfies the congruence $\omega \equiv 1 \pmod{\mathfrak{l}}$ then, if

$$\omega = c + c_1\zeta + \cdots + c_{l-2}\zeta^{l-2},$$

where $c, c_1, \ldots, c_{l-2}$ are rational integers, we have the congruence

$$c + c_1 + \cdots + c_{l-2} \equiv 1 \pmod{l}.$$

We now define

$$\omega(x) = c + c_1x + \cdots + c_{l-2}x^{l-2} - \frac{c + c_1 + \cdots + c_{l-2} - 1}{l}(1 + x + \cdots + x^{l-1}).$$

Then $\omega(x)$ is an integer polynomial of degree $l-1$ and we have

$$\omega(1) = 1 \quad \text{and} \quad \omega(\zeta) = \omega.$$

We call $\omega(x)$ the *function belonging to* the integer ω. We shall also write

$$\left[\frac{d^g \log\omega(e^v)}{dv^g}\right]_{v=0} = \mathrm{l}^{(g)}(\omega) \tag{29.10}$$

for $g = 1, 2, \ldots, l-1$; this notation, introduced by Kummer, has the advantage of abbreviating some calculations (*Kummer* (12)).

If a number ω which is congruent to 1 modulo $\mathfrak{l}$ is expressed in any way in the form

$$\omega = a + a_1\zeta + \cdots + a_t\zeta^t,$$

where $a, a_1, \ldots, a_t$ are rational integers, then

$$\bar{\omega}(x) = a + a_1x + \cdots + a_tx^t$$

is an integer polynomial of degree t which in general does not satisfy the equation $\bar{\omega}(1) = 1$ but only the congruence

$$\bar{\omega}(1) \equiv 1 \pmod{l}$$

and so is prime to l for $x = 1$. We have the following congruences between the derivatives of $\log\bar{\omega}(e^v)$ for $v = 0$ and the derivatives introduced in (29.10):

$$\left[\frac{d^g \log\bar{\omega}(e^v)}{dv^g}\right]_{v=0} \equiv \mathrm{l}^{(g)}(\omega) \pmod{l}$$

for $g = 1, 2, \ldots, l-2$ and

$$\left[\frac{d^{l-1} \log\bar{\omega}(e^v)}{dv^{l-1}}\right]_{v=0} \equiv \mathrm{l}^{(l-1)}(\omega) + \frac{1-\bar{\omega}(1)}{l} \pmod{l}.$$

These congruences follow easily when we remark that

$$\omega(x) = \bar{\omega}(x) + \frac{1-\bar{\omega}(1)}{l}(1 + x + \cdots + x^{l-1}) + O(x)(x^l - 1)$$

and

$$\omega(e^v) \equiv \bar{\omega}(e^v) + \frac{1-\bar{\omega}(1)}{l} v^{l-1} \pmod{l},$$

where in the first formula $O(x)$ is a certain integer polynomial in x and the second formula is taken to mean that in the expansion in powers of v of both sides of the congruence the coefficients of $1, v, v^2, \ldots, v^{l-1}$ are congruent modulo l.

If ν and μ are integers of $k(\zeta)$ such that $\nu \equiv 1$, $\mu \equiv 1 \pmod{\mathfrak{l}}$ we define the symbol $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ as follows:

$$\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\} = \zeta^{\mathrm{l}^{(1)}(\nu)\mathrm{l}^{(l-1)}(\mu) - \mathrm{l}^{(2)}(\nu)\mathrm{l}^{(l-2)}(\mu) + \cdots - \mathrm{l}^{(l-1)}(\nu)\mathrm{l}^{(1)}(\mu)}. \tag{29.11}$$

From this definition we deduce at once the following rules:

$$\left.\begin{aligned} \left\{\frac{\nu_1\nu_2, \mu}{\mathfrak{l}}\right\} &= \left\{\frac{\nu_1, \mu}{\mathfrak{l}}\right\}\left\{\frac{\nu_2, \mu}{\mathfrak{l}}\right\} \\ \left\{\frac{\nu, \mu_1\mu_2}{\mathfrak{l}}\right\} &= \left\{\frac{\nu, \mu_1}{\mathfrak{l}}\right\}\left\{\frac{\nu, \mu_2}{\mathfrak{l}}\right\} \\ \left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}\left\{\frac{\mu, \nu}{\mathfrak{l}}\right\} &= 1 \end{aligned}\right\} \tag{29.12}$$

where $\nu, \nu_1, \nu_2, \mu, \mu_1, \mu_2$ are any integers of $k(\zeta)$ congruent to 1 modulo $\mathfrak{l}$. If r is a primitive root modulo l and $s = (\zeta : \zeta^r)$ the corresponding automorphism in the group of the cyclotomic field $k(\zeta)$ then, as is easily seen, we have the further formula

$$\left\{\frac{s\nu, s\mu}{\mathfrak{l}}\right\} = \left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}^r. \tag{29.13}$$

If ν and μ are any integers of $k(\zeta)$ prime to $\mathfrak{l}$ then we define the symbol $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ by

$$\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\} = \left\{\frac{\nu^{l-1}, \mu^{l-1}}{\mathfrak{l}}\right\}.$$

For the case where one or both of the numbers ν, μ is divisible by $\mathfrak{l}$ we refer to the remarks at the end of Sect. 133.

§132. Some Lemmas on the Symbol $\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}$ and Norm Residues Modulo the Prime Ideal $\mathfrak{l}$

Lemma 24 (*Kummer* (20)). *Let ω be an integer of $k(\zeta)$ such that $\omega \equiv 1$ (mod $\mathfrak{l}$). Then the norm $n(\omega)$ satisfies the congruence*

$$\mathrm{l}^{(l-1)}(\omega) \equiv \frac{1-n(\omega)}{l} \pmod{l}.$$

Proof. Let $\omega(x)$ be the function belonging to ω and set

$$F(x) = \prod_{(g)} \omega(1 + x(\zeta^g - 1))$$

where the product is taken over the values $g = 0, 1, 2, \ldots, l-1$. The expression $F(x)$ is an integer polynomial in x and the coefficients of all the terms of this polynomial divisible by x^l are obviously divisible by λ^l and so, since the coefficients are rational, by l^2. Expanding by powers of x we have

$$\left.\begin{aligned} \log\omega(1 + x(\xi - 1)) &= \frac{\xi - 1}{1!}x\left[\frac{d\log\omega(x)}{dx}\right]_{x=1} \\ &\quad + \frac{(\xi-1)^2}{2!}x^2\left[\frac{d^2\log\omega(x)}{dx^2}\right]_{x=1} + \cdots \\ &\quad + \cdots + \frac{(\xi-1)^{l-1}}{(l-1)!}x^{l-1}\left[\frac{d^{l-1}\log\omega(x)}{dx^{l-1}}\right]_{x=1} + \cdots \end{aligned}\right\} \quad (29.14)$$

In this expansion we first substitute in succession

$$\xi = 1, \zeta, \zeta^2, \ldots, \zeta^{l-1}$$

and add the results; using the fact that

$$(\zeta - 1)^g + (\zeta^2 - 1)^g + \cdots + (\zeta^{l-1} - 1)^g = (-1)^g l \quad (g = 1, 2, \ldots, l-1)$$

we obtain the equation

$$\left.\begin{aligned} \log F(x) &= l\left\{-\frac{x}{1!}\left[\frac{d\log\omega(x)}{dx}\right]_{x=1}\right. \\ &\quad + \frac{x^2}{2!}\left[\frac{d^2\log\omega(x)}{dx^2}\right]_{x=1} - \cdots \\ &\quad \left.\cdots + \frac{x^{l-1}}{(l-1)!}\left[\frac{d^{l-1}\log\omega(x)}{dx^{l-1}}\right]_{x=1}\right\} + x^l G \end{aligned}\right\} \quad (29.15)$$

where $x^l G$ is the sum of all the terms of the expansion divisible by x^l.

Secondly, we substitute $\xi = e^v$ in equation (29.14) and form the $(l-1)$-st derivative with respect to v. Then, evaluating at $v = 0$, we have

$$\left.\begin{aligned}
&\left[\frac{d^{l-1}\log\omega(1+x(e^v-1))}{dv^{l-1}}\right]_{v=0} = \frac{x}{1!}\left[\frac{d\log\omega(x)}{dx}\right]_{x=1}\\
&\quad+\frac{2^{l-1}-2\cdot 1^{l-1}}{2!}x^2\left[\frac{d^2\log\omega(x)}{dx^2}\right]_{x=1}\\
&\quad+\frac{3^{l-1}-3\cdot 2^{l-1}+3\cdot 1^{l-1}}{3!}x^3\left[\frac{d^3\log\omega(x)}{dx^3}\right]_{x=1}+\cdots\\
&\quad+\frac{(l-1)^{l-1}-\cdots-(l-1)\cdot 1^{l-1}}{(l-1)!}x^{l-1}\left[\frac{d^{l-1}\log\omega(x)}{dx^{l-1}}\right]_{x=1}\\
&\quad\equiv \frac{x}{1!}\left[\frac{d\log\omega(x)}{dx}\right]_{x=1}-\frac{x^2}{2!}\left[\frac{d^2\log\omega(x)}{dx^2}\right]_{x=1}+\cdots\\
&\qquad\cdots-\frac{x^{l-1}}{(l-1)!}\left[\frac{d^{l-1}\log\omega(x)}{dx^{l-1}}\right]_{x=1} \pmod{l}.
\end{aligned}\right\} \tag{29.16}$$

Combining the formulae (29.15) and (29.16) we have

$$\log F(x) \equiv -l\left[\frac{d^{l-1}\log\omega(1+x(e^v-1))}{dv^{l-1}}\right]_{v=0} \pmod{l^2}$$

in the sense that the coefficients of x, x^2, ..., x^{l-1} on the left hand side are congruent modulo l^2 to the corresponding coefficients on the right hand side. If we take the exponential of both sides of this congruence then we obtain first in the same sense and then, having regard to the remark made at the beginning of this proof, completely, the congruence of the two integer polynomials

$$F(x) \equiv 1-l\left[\frac{d^{l-1}\log\omega(1+x(e^v-1))}{dv^{l-1}}\right]_{v=0} \pmod{l^2}$$

and hence, setting $x=1$, we have

$$n(\omega) \equiv 1-l\cdot \mathfrak{l}^{(l-1)}(\omega) \pmod{l^2}.$$

This completes the proof of Lemma 24.

Lemma 25. *Let ν and μ be integers of $k(\zeta)$ such that $\nu \equiv 1 \pmod{\mathfrak{l}}$ and $\mu \equiv 1+\lambda \pmod{\mathfrak{l}^2}$. If ν is congruent modulo $\mathfrak{l}^l$ to the relative norm of an integer A of the Kummer field $k(\mathsf{M},\zeta)$ determined by $\mathsf{M}=\sqrt[l]{\mu}$ then there exists an integer polynomial $f(x)$ of degree $l-1$ in x such that $f(1)>0$ satisfying the congruences*

$$n(f(\zeta)) \equiv 1 \pmod{l^2}$$

and

$$\nu \equiv f(\mu) \pmod{\mathfrak{l}^l}$$

(*Kummer* (20)).

Proof. According to the proof of Lemma 23 every integer A in $k(\mathsf{M},\zeta)$ can be expressed in the form

$$\mathsf{A} = \frac{\gamma + \gamma_1(\mathsf{M}-1) + \cdots + \gamma_{l-1}(\mathsf{M}-1)^{l-1}}{\delta}$$

and hence in the form

$$\mathsf{A} = \frac{\beta + \beta_1\mathsf{M} + \cdots + \beta_{l-1}\mathsf{M}^{l-1}}{\delta}$$

where γ, γ_1, ..., γ_{l-1}, δ and β, β_1, ..., β_{l-1} are integers of $k(\zeta)$ and δ is prime to $\mathfrak{l}$. From the latter result we see that we can write

$$\mathsf{A} \equiv \alpha + \alpha_1\mathsf{M} + \cdots + \alpha_{l-1}\mathsf{M}^{l-1} \pmod{\mathfrak{l}^l}$$

where α, α_1, ..., α_{l-1} are integers in $k(\zeta)$. Suppose now that

$$\alpha \equiv a^*, \quad \alpha_1 \equiv a_1^*, \quad \ldots \quad, \alpha_{l-1} \equiv a_{l-1}^* \pmod{\mathfrak{l}}$$

where a^*, a_1^*, ..., a_{l-1}^* are positive rational integers. We set

$$f^*(x) = a^* + a_1^* x + \cdots + a_{l-1}^* x^{l-1}.$$

Since we have $\mathfrak{l} = \mathfrak{L}^l$ and $\mathsf{M} \equiv 1 \pmod{\mathfrak{L}}$ in $k(\mathsf{M},\zeta)$ it follows that

$$\mathsf{A} \equiv \alpha + \alpha_1 + \cdots + \alpha_{l-1} \equiv a^* + a_1^* + \cdots + a_{l-1}^* \pmod{\mathfrak{L}}.$$

If now A is the number mentioned in the statement of the lemma such that $\nu \equiv N_k(\mathsf{A}) \pmod{\mathfrak{l}^l}$ then we have further that

$$\nu \equiv N_k(\mathsf{A}) \equiv a^* + a_1^* + \cdots + a_{l-1}^* \equiv 1 \pmod{\mathfrak{L}}$$

and hence also that

$$a^* + a_1^* + \cdots + a_{l-1}^* \equiv 1 \pmod{l}. \tag{29.17}$$

It follows that $f^*(\zeta)$ is a number in $k(\zeta)$ satisfying the congruence $f^*(\zeta) \equiv 1 \pmod{\mathfrak{l}}$. From this it is easy to find a positive rational integer b such that the norm of the number $f(\zeta) = f^*(\zeta) + lb$ in $k(\zeta)$ satisfies the congruence

$$n(f(\zeta)) \equiv 1 \pmod{l^2}. \tag{29.18}$$

Then the integer polynomial

$$f(x) = f^*(x) + lb = a + a_1 x + \cdots + a_{l-1} x^{l-1}$$

satisfies the requirements of Lemma 25. For it is clear that $\mathsf{A} = f(\mathsf{M}) + \lambda\mathsf{B}$, where B is an integer in $k(\mathsf{M}, \zeta)$. From this we deduce, using an argument similar to that on p. 239, that

$$\nu \equiv N_k(\mathsf{A}) \equiv N_k(f(\mathsf{M})) \pmod{\mathfrak{l}^l}. \tag{29.19}$$

On the other hand, by considering the congruences

$$a^l \equiv a, \quad a_1^l \equiv a_1, \quad \dots \quad , a_{l-1}^l \equiv a_{l-1} \pmod{l},$$

we see that we have

$$f(x)f(\zeta x)\cdots f(\zeta^{l-1}x) = f(x^l) + lF(x^l), \tag{29.20}$$

identically in x, where $F(x^l)$ is a polynomial in x^l with integer coefficients. Using (29.18) we see that when we set $x = 1$ we have the congruence

$$f(1) \equiv f(1) + lF(1) \pmod{l^2},$$

whence

$$F(1) \equiv 0 \pmod{l}.$$

If we set $x = \mathsf{M}$ in equation (29.20) we obtain

$$N_k(f(\mathsf{M})) = f(\mu) + lF(\mu)$$

and hence, since $F(\mu) \equiv F(1) \equiv 0 \pmod{\mathfrak{l}}$,

$$N_k(f(\mathsf{M})) \equiv f(\mu) \pmod{\mathfrak{l}^l};$$

so, by (22.19),

$$\nu \equiv f(\mu) \pmod{\mathfrak{l}^l}.$$

This result together with (29.18) completes the proof of Lemma 25.

Lemma 26. *Let ν and μ be integers of $k(\zeta)$ such that $\nu \equiv 1 \pmod{\mathfrak{l}}$ and $\mu \equiv 1 + \lambda \pmod{\mathfrak{l}^2}$. If ν is a norm residue modulo $\mathfrak{l}$ of the Kummer field $k(\mathsf{M}, \zeta)$ determined by $\mathsf{M} = \sqrt[l]{\mu}$ then*

$$\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\} = 1$$

(*Kummer* (20)).

Proof. Let $F(v)$ be an arbitrary power series in v and $\varphi(v)$ a power series in v with nonzero constant term. If the variables v and V are related by the condition that $V\varphi(v) - v = 0$ then Lagrange's formula for the reversion of power series yields the following identity

$$\left[\frac{d^{l-1}F(v)}{dV^{l-1}}\right]_{V=0} = \left[\frac{d^{l-2}\frac{dF(v)}{dv}(\varphi(v))^{l-1}}{dv^{l-2}}\right]_{v=0}. \tag{29.21}$$

Now let $\nu(x)$ and $\mu(x)$ be the functions belonging to the numbers ν and μ respectively. Since ν is a norm residue modulo $\mathfrak{l}$ of the field $k(\mathsf{M},\zeta)$ it follows from Lemma 25 that there is an integer polynomial $f(x)$ of degree $l-1$ such that

$$n(f(\zeta)) \equiv 1 \pmod{l^2}, \tag{29.22}$$

$$\nu \equiv f(\mu) \pmod{\mathfrak{l}^l} \tag{29.23}$$

and $f(1) > 0$.

We set

$$F(v) = \log f(\mu(e^v)),$$
$$V = \log \mu(e^v),$$
$$\varphi(v) = \frac{v}{\log \mu(e^v)}.$$

These functions will be considered only at the place $v = 0$ and the logarithms chosen so that they take real values at $v = 0$.

In the formula for $\left[\frac{d^{l-1}\log\bar{\omega}(e^v)}{dv^g}\right]_{v=0}$ on p. 241 we replace the symbols ω, $\bar{\omega}(x)$ and v by $f(\zeta)$, $f(x)$ and V respectively, obtaining

$$\left[\frac{d^{l-1}\log f(e^V)}{dV^{l-1}}\right]_{V=0} \equiv \mathrm{l}^{(l-1)}(f(\zeta)) + \frac{1-f(1)}{l} \pmod{l}.$$

When we use (29.22) Lemma 24 yields the congruence

$$\mathrm{l}^{(l-1)}(f(\zeta)) \equiv 0 \pmod{l}$$

and consequently

$$\left[\frac{d^{l-1}F(v)}{dV^{l-1}}\right]_{V=0} \equiv \left[\frac{d^{l-1}\log f(e^V)}{dV^{l-1}}\right]_{V=0} \equiv \frac{1-f(1)}{l} \pmod{l}. \tag{29.24}$$

On the other hand, when we take account of (29.23) we have the congruence

$$f(\mu(e^v)) \equiv \nu(e^v) + \frac{f(1)-1}{l}v^{l-1} \pmod{l}$$

which is to be understood in the sense that when both sides are expanded in powers of v the coefficients of $1, v, \ldots, v^{l-1}$ in the two expansions are congruent modulo l; from this we have the expansion

$$\begin{aligned}\frac{dF(v)}{dv} \equiv \mathrm{l}^{(1)}(\nu) + \mathrm{l}^{(2)}(\nu)\frac{v}{1!} + \mathrm{l}^{(3)}(\nu)\frac{v^2}{2!} + \cdots \\ + \left(\mathrm{l}^{(l-1)}(\nu) + \frac{1-f(1)}{l}\right)\frac{v^{l-2}}{(l-2)!} \pmod{l},\end{aligned} \tag{29.25}$$

which is to be understood as asserting that the coefficients of $1, v, \ldots, v^{l-2}$ on the two sides are congruent modulo l.

Finally we consider the function $\varphi(v)$. Since $\mu \equiv 1 + \lambda \pmod{\mathfrak{l}^2}$, $\varphi(v)$ is a power series whose constant term is congruent to -1 modulo l. Further, it follows easily that

$$-(\varphi(v))^l \equiv \varphi(v^l) \equiv \varphi(0) \equiv -1 \pmod{l}$$

in the sense that the coefficients of $1, v, \ldots, v^{l-2}$ on the two sides are congruent modulo l. From this it follows that, in the same sense,

$$-\varphi(v)^{l-1} \equiv \frac{\log \mu(e^v)}{v} \pmod{l}$$

and from this we have (still in the same sense) the expansion

$$\begin{aligned} -(\varphi(v))^{l-1} \equiv \mathfrak{l}^{(1)}(\mu) + \mathfrak{l}^{(2)}(\mu)\frac{v}{2!} + \mathfrak{l}^{(3)}(\mu)\frac{v^2}{3!} + \cdots \\ + \mathfrak{l}^{(l-1)}(\mu)\frac{v^{l-2}}{(l-1)!} \pmod{l}. \end{aligned} \tag{29.26}$$

Combining the congruences (29.24) and the expansions (29.25) and (29.26) with the equation (29.21) and using the facts that $\mathfrak{l}^{(1)}(\mu) \equiv -1$ and $(l-g)!(g-1)! \equiv (-1)^g \pmod{l}$ for $g = 1, 2, \ldots, l-1$, we obtain the following congruence:

$$\mathfrak{l}^{(l-1)}(\nu)\mathfrak{l}^{1)}(\mu) - \mathfrak{l}^{(l-2)}(\nu)\mathfrak{l}^{(2)}(\mu) + \cdots - \mathfrak{l}^{(1)}(\nu)\mathfrak{l}^{(l-1)}(\mu) \equiv 0 \pmod{l}.$$

Hence, according to the definition (29.11) of the symbol $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ in Sect. 131, we have

$$\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\} = 1.$$

This completes the proof of Lemma 26.

§133. Use of the Symbol $\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\}$ to Distinguish Norm Residues and Non-residues

We are now in a position to establish the following assertion in the cases where the symbols involved have already been defined.

Theorem 151. *Let ν and μ be any two integers of the cyclotomic field $k(\zeta)$ subject only to the condition that $\sqrt[l]{\mu}$ does not belong to $k(\zeta)$; let $\mathfrak{w}$ be any prime ideal of $k(\zeta)$. Then ν is a norm residue or non-residue modulo $\mathfrak{w}$ of the Kummer field $k(\mathsf{M}, \zeta)$ determined by $\mathsf{M} = \sqrt[l]{\mu}$ according as $\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\} = 1$ or $\neq 1$.*

Proof. First let $\mathfrak{w}$ be a prime ideal distinct from $\mathfrak{l}$ which does not divide the relative discriminant of the field $k(\mathsf{M},\zeta)$. If μ^* is an integer in $k(\zeta)$ such that μ^*/μ is the l-th power of a number in $k(\zeta)$ then we have $\left\{\frac{\nu,\mu^*}{\mathfrak{w}}\right\} = \left\{\frac{\nu,\mu}{\mathfrak{w}}\right\}$. Hence, having regard to Theorem 148, we may suppose that μ is not divisible by $\mathfrak{w}$. We distinguish two cases, according as $\mathfrak{w}$ splits in $k(\mathsf{M},\zeta)$ as the product of l prime ideals $\mathfrak{W}_1, \ldots, \mathfrak{W}_l$ or remains a prime ideal in $k(\mathsf{M},\zeta)$. According to Theorem 149, in the first case we have $\left\{\frac{\mu}{\mathfrak{w}}\right\} = 1$ and in the second case $\left\{\frac{\mu}{\mathfrak{w}}\right\} \neq 1$ and $\neq 0$.

In the first case we find an integer A of $k(\mathsf{M},\zeta)$ which is divisible by $\mathfrak{W}_1$ but not by $\mathfrak{W}_1^2$ nor by any of the prime ideals $\mathfrak{W}_2, \ldots, \mathfrak{W}_l$. Then the prime ideal $\mathfrak{w}$ occurs as a factor of $\alpha = N_k(\mathsf{A})$ to the first power precisely. If $\mathfrak{w}^b$ is the highest power of $\mathfrak{w}$ dividing ν then $\kappa = \nu/\alpha^b$ can be written as a fraction whose numerator and denominator are prime to $\mathfrak{w}$; hence, according to Theorem 150, the numerator and denominator of this fraction are norm residues modulo $\mathfrak{w}$ of the field $k(\mathsf{M},\zeta)$. Hence the same holds for ν. According to the definition in Sect. 131,

$$\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\} = \left\{\frac{\mu^b}{\mathfrak{w}}\right\}^{-1} = 1$$

and so in this first case Theorem 151 is established.

In the second case the exponent of the precise power of $\mathfrak{w}$ dividing the relative norm of an integer A of $k(\mathsf{M},\zeta)$ is divisible by l. Again let $\mathfrak{w}^b$ be the highest power of $\mathfrak{w}$ dividing ν. If b is not a multiple of l then ν cannot be a norm residue modulo $\mathfrak{w}$; in this case we have $\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\} = \left\{\frac{\mu^b}{\mathfrak{w}}\right\}^{-1} \neq 1$. If, on the other hand, b is a multiple of l then we take α to be an integer of $k(\zeta)$ divisible by $\mathfrak{w}$ but not by $\mathfrak{w}^2$ and set $\kappa = \nu/\alpha^b$; as in the first case ν is a norm residue modulo $\mathfrak{w}$ and we have $\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\} = \left\{\frac{\mu^b}{\mathfrak{w}}\right\}^{-1} = 1$. Thus we have proved Theorem 151 for the second case also.

Now we suppose that $\mathfrak{w}$ is a prime ideal distinct from $\mathfrak{l}$ which divides the relative discriminant of the field $k(\mathsf{M},\zeta)$. Suppose the precise powers of $\mathfrak{w}$ dividing ν and μ are $\mathfrak{w}^b$ and $\mathfrak{w}^a$ respectively; a is not a multiple of l. The number $\kappa = \nu^a/\mu^b$ can be expressed as a fraction ρ/σ whose numerator ρ and denominator σ are prime to $\mathfrak{w}$. The number $\rho\sigma^{l-1}$ is an integer not divisible by $\mathfrak{w}$; according to the proof of Theorem 150 on p. 236 such an integer is a norm residue modulo $\mathfrak{w}$ of the field $k(\mathsf{M},\zeta)$ if and only if it is an l-th power residue modulo $\mathfrak{w}$, i.e. in the present situation if and only if $\left\{\frac{\rho\sigma^{l-1}}{\mathfrak{w}}\right\} = 1$ and so $\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\} = 1$. Thus in the case at present under consideration we have again established Theorem 151.

Finally let $\mathfrak{w} = \mathfrak{l}$. We consider only the case in which $\mu \equiv 1 + \lambda$ (mod $\mathfrak{l}^2$): this is the only case of the theorem which we shall need later

on; the other cases, however, yield to a similar treatment. For the proof we shall suppose that $\nu \equiv 1 \pmod{\mathfrak{l}}$, which is no essential restriction. According to our assumption that $\mu \equiv 1+\lambda \pmod{\mathfrak{l}^2}$ we deduce from Theorem 150 that there are precisely l^{l-1} norm residues ν^* modulo $\mathfrak{l}$ of the field $k(\mathsf{M},\zeta)$ which are congruent to 1 modulo $\mathfrak{l}$ and mutually incongruent modulo $\mathfrak{l}^{l+1}$. On the other hand it follows from Lemma 26 that each norm residue ν^* modulo $\mathfrak{l}$ of $k(\mathsf{M},\zeta)$ for which $\nu^* \equiv 1 \pmod{\mathfrak{l}}$ must satisfy the condition $\left\{\frac{\nu^*,\mu}{\mathfrak{l}}\right\} = 1$. Since

$$\left.\begin{array}{rcl} \mathrm{l}^{(1)}(\mu) & \equiv & -1 \\ \mathrm{l}^{(1)}(1-l) & \equiv & 0,\ \ \mathrm{l}^{(2)}(1-l) \equiv 0,\ \ \ldots\ ,\ \ \mathrm{l}^{(l-2)}(1-l) \equiv 0, \\ \mathrm{l}^{(l-1)}(1-l) & \equiv & \dfrac{1-n(1-l)}{l} \equiv -1, \end{array}\right\} \pmod{l}$$

it follows from (29.11) that

$$\left\{\frac{1-l,\mu}{\mathfrak{l}}\right\} = \zeta^{-1}. \tag{29.27}$$

First let α be any integer of $k(\zeta)$ such that $\alpha \equiv 1 \pmod{\mathfrak{l}}$ and suppose that $\left\{\frac{\alpha,\mu}{\mathfrak{l}}\right\} = \zeta^a$, where a is an integer in the range $0, 1, 2, \ldots, l-1$. Then obviously $\left\{\frac{\alpha(1-l)^a,\mu}{\mathfrak{l}}\right\} = 1$ but $\left\{\frac{\alpha(1-l)^x,\mu}{\mathfrak{l}}\right\} \neq 1$ if x is any integer distinct from a in the range $0, 1, 2, \ldots, l-1$. Next let α' be an integer of $k(\zeta)$ which is congruent to 1 modulo $\mathfrak{l}$ but not congruent modulo $\mathfrak{l}^{l+1}$ to any of the l numbers $\alpha, \alpha(1-l), \alpha(1-l)^2, \ldots, \alpha(1-l)^{l-1}$. Then the l numbers $\alpha', \alpha'(1-l), \alpha'(1-l)^2, \ldots, \alpha'(1-l)^{l-1}$ are all mutually incongruent modulo $\mathfrak{l}^{l+1}$ and furthermore none of them is congruent to any of the first l numbers. Using (29.27) we see that among the latter l numbers there is clearly one and only one, say $\alpha'(1-l)^{a'}$, such that $\left\{\frac{\alpha'(1-l)^{a'},\mu}{\mathfrak{l}}\right\} = 1$. Proceeding in this way we see that there are precisely l^{l-1} numbers ν, mutually incongruent modulo $\mathfrak{l}^{l+1}$, which are congruent to 1 modulo $\mathfrak{l}$ and satisfy the condition that $\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\} = 1$. Since this is the same as the number of norm residues ν^* found above, it is clear that, conversely, every number ν with the two properties is a norm residue modulo $\mathfrak{l}$ of the field $k(\mathsf{M},\zeta)$.

The preceding arguments serve to establish all parts of Theorem 151, although in the case where $\mathfrak{w} = \mathfrak{l}$ we have considered only the case where ν and μ satisfy the conditions $\nu \equiv 1 \pmod{\mathfrak{l}}$ and $\mu \equiv 1+\lambda \pmod{\mathfrak{l}^2}$. The restriction on ν is clearly easily removed.

Using Theorem 151 we deduce from the first formulæ in (29.9) and (29.12) that

$$\left\{\frac{\nu\nu^*,\mu}{\mathfrak{w}}\right\} = \left\{\frac{\nu,\mu}{\mathfrak{w}}\right\}$$

where $\mathfrak{w}$ is any prime ideal in $k(\zeta)$ and ν^* is a norm residue modulo $\mathfrak{w}$ of $k(\mathsf{M},\zeta)$.

In order to define the symbol $\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}$ in the case where one or both of the numbers ν, μ is divisible by $\mathfrak{l}$ we need only require the general validity of the formulae

$$\left\{\frac{\nu\nu^*,\mu}{\mathfrak{l}}\right\} = \left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}, \quad \left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}\left\{\frac{\mu,\nu}{\mathfrak{l}}\right\} = 1$$

where ν^* is any norm residue modulo $\mathfrak{l}$ of the field $k(\sqrt[l]{\mu},\zeta)$. From this stipulation we deduce in particular that

$$\left\{\frac{1+a\lambda^l,\lambda}{\mathfrak{l}}\right\} = \left\{\frac{1+a\lambda^l}{\mathfrak{l}}\right\} = \zeta^a.$$

We can base the definition of the symbol $\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}$ on the formulæ

$$\left\{\frac{\alpha,\zeta}{\mathfrak{l}}\right\} = \zeta^{(n(\alpha)-1)/l}, \quad \left\{\frac{\nu_1\nu_2,\mu}{\mathfrak{l}}\right\} = \left\{\frac{\nu_1,\mu}{\mathfrak{l}}\right\}\left\{\frac{\nu_2,\mu}{\mathfrak{l}}\right\},$$

$$\left\{\frac{\nu^*,\mu}{\mathfrak{l}}\right\} = 1, \quad \left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}\left\{\frac{\mu,\nu}{\mathfrak{l}}\right\} = 1,$$

where α is an integer of $k(\zeta)$ prime to $\mathfrak{l}$, ν^* is a norm residue modulo $\mathfrak{l}$ of the field $k(\sqrt[l]{\mu},\zeta)$ and ν, ν_1, ν_2, μ are any integers in $k(\zeta)$ (see Sect. 166). I have, however, chosen here the definition (29.11) above, which ties up directly with Kummer's development.

Finally we remark that the goal we set ourselves at the beginning of Sect. 131 has now been achieved; namely, if $\mathfrak{w}^e$ is any power of the prime ideal $\mathfrak{w}$ (where, in the case $\mathfrak{w} = \mathfrak{l}$ the exponent e exceeds l) then a complete set of numbers ν in $k(\zeta)$ prime to $\mathfrak{w}$ and mutually incongruent modulo $\mathfrak{w}^e$ can be partitioned into l equinumerous subsets according to the values assumed by the symbol $\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\}$; one of these subsets consists of all the norm residues modulo $\mathfrak{w}$ of the Kummer field $k(\mathsf{M},\zeta)$ which occur in the original set.

30. Existence of Infinitely Many Prime Ideals with Prescribed Power Characters in a Kummer Field

§134. The Limit of a Certain Infinite Product

Having determined in Sect. 128 all the prime ideals of a Kummer field we are in a position to carry out for Kummer fields investigations corresponding to the questions which we discussed in Sect. 79 and Sect. 80 in the case of quadratic fields . We derive first the following important result.

Lemma 27. *Let l be an odd rational prime number and α an integer in the cyclotomic field $k(\zeta)$ generated by $\zeta = e^{2\pi i/l}$ which is not the l-th power of a number in $k(\zeta)$. Then the limit*

$$\lim_{s=1} \prod_{(\mathfrak{p})} \prod_{(m)} \frac{1}{1 - \left\{\frac{\alpha}{\mathfrak{p}}\right\} n(\mathfrak{p})^{-s}}$$

is finite and nonzero. (The product $\prod\limits_{(\mathfrak{p})}$ is taken over all prime ideals $\mathfrak{p}$ of the field $k(\zeta)$ and the product $\prod\limits_{(m)}$ over all exponents m in the range 1, 2, ..., $l-1$.) (*Kummer* (20)).

Proof. We consider the Kummer field $K = k(\sqrt[l]{\alpha}, \zeta)$ generated by $\sqrt[l]{\alpha}$ and ζ and denote by $\zeta_K(s)$ the function $\zeta(s)$ for K defined as in Theorem 56. Then, according to Sect. 27, we have

$$\zeta_K(s) = \prod_{\mathfrak{P}} \frac{1}{1 - N(\mathfrak{P})^{-s}},$$

where the product is taken over all prime ideals $\mathfrak{P}$ of K and $N(\mathfrak{P})$ is the norm of $\mathfrak{P}$ in K. We arrange the product according to the prime ideals $\mathfrak{p}$ of $k(\zeta)$ from which the prime ideals $\mathfrak{P}$ are derived: we conclude from Theorem 149 that to each prime ideal $\mathfrak{p}$ there corresponds as a factor of the product either

$$\frac{1}{(1 - n(\mathfrak{p})^{-s})^l} \quad \text{or} \quad \frac{1}{1 - n(\mathfrak{p})^{-s}} \quad \text{or} \quad \frac{1}{1 - n(\mathfrak{p})^{-ls}}$$

according as $\left\{\frac{\alpha}{\mathfrak{p}}\right\} = 1$ or $= 0$ or is distinct from 0 and 1. We write these expressions in the common form

$$\frac{1}{1-n(\mathfrak{p})^{-s}} \prod_{(m)} \frac{1}{1-\left\{\frac{\alpha}{\mathfrak{p}}\right\}^m n(\mathfrak{p})^{-s}} \qquad (m = 1, 2, \ldots, l-1)$$

and so obtain

$$\zeta_K(s) = \prod_{(\mathfrak{p})} \frac{1}{1-n(\mathfrak{p})^{-s}} \prod_{(\mathfrak{p})} \prod_{(m)} \frac{1}{1-\left\{\frac{\alpha}{\mathfrak{p}}\right\}^m n(\mathfrak{p})^{-s}} \tag{30.1}$$

where the product $\prod_{(m)}$ runs over the exponents 1, 2, ..., $l-1$ and both products $\prod_{(\mathfrak{p})}$ run over all prime ideals $\mathfrak{p}$ of $k(\zeta)$. Now both expressions

$$\lim_{s=1} (s-1) \prod_{(\mathfrak{p})} \frac{1}{1-n(\mathfrak{p})^{-s}} \quad \text{and} \quad \lim_{s=1} (s-1)\zeta_K(s)$$

are finite and nonzero, as we see when we apply Theorem 56 once to the cyclotomic field $k(\zeta)$ and then to the Kummer field $K = k(\sqrt[l]{\alpha}, \zeta)$. When we multiply (30.1) by $s-1$ and take the limit at $s = 1$ we see that the expression given in Lemma 27 is also finite and nonzero.

§135. Prime Ideals of the Cyclotomic Field $k(\zeta)$ with Prescribed Power Characters

Theorem 152. *Let $\alpha_1, \ldots, \alpha_t$ be any t integers of the cyclotomic field $k(\zeta)$ such that none of the products*

$$\alpha_1^{m_1} \alpha_2^{m_2} \cdots \alpha_t^{m_t}$$

(where $m_1, m_2, \ldots, m_t$ run through the range $0, 1, \ldots, l-1$), except when $m_1 = m_2 = \ldots = m_t = 0$, is the l-th power of a number in $k(\zeta)$. Let $\gamma_1, \gamma_2, \ldots, \gamma_t$ be arbitrarily chosen l-th roots of unity. Then there are infinitely many prime ideals $\mathfrak{p}$ of the cyclotomic field $k(\zeta)$ for which

$$\left\{\frac{\alpha_1}{\mathfrak{p}}\right\}^m = \gamma_1, \left\{\frac{\alpha_2}{\mathfrak{p}}\right\}^m = \gamma_2, \ldots, \left\{\frac{\alpha_t}{\mathfrak{p}}\right\}^m = \gamma_t$$

for some exponent m prime to l (Kummer (20)).

Proof. If $s > 1$ we have

$$\left.\begin{aligned}\log \sum_{(\mathfrak{i})} \frac{1}{n(\mathfrak{i})^s} &= \sum_{(\mathfrak{p})} \log \frac{1}{1-n(\mathfrak{p})^{-s}} = \sum_{(\mathfrak{p})} \frac{1}{n(\mathfrak{p})^s} + S, \\ S &= \tfrac{1}{2}\sum_{(\mathfrak{p})} \frac{1}{n(\mathfrak{p})^{2s}} + \tfrac{1}{3}\sum_{(\mathfrak{p})} \frac{1}{n(\mathfrak{p})^{3s}} + \cdots\end{aligned}\right\} \quad (30.2)$$

where $\sum\limits_{(\mathfrak{i})}$ runs over all ideals $\mathfrak{i}$ and each sum $\sum\limits_{(\mathfrak{p})}$ runs over all the prime ideals of the field $k(\zeta)$. Since the expression S, as was shown in Sect. 50, remains finite for $s = 1$, it follows from (30.2), in which the left hand side is infinite for $s = 1$, that the sum

$$\sum_{(\mathfrak{p})} \frac{1}{n(\mathfrak{p})^s}$$

taken over all prime ideals $\mathfrak{p}$ of $k(\zeta)$ increases beyond all bounds as s approaches 1. If α is any integer of $k(\zeta)$ then in a similar way we have for $s > 1$

$$\left.\begin{aligned}\log \prod_{(\mathfrak{p})} \frac{1}{1-\left\{\frac{\alpha}{\mathfrak{p}}\right\} n(\mathfrak{p})^{-s}} &= \sum_{(\mathfrak{p})} \left\{\frac{\alpha}{\mathfrak{p}}\right\} \frac{1}{n(\mathfrak{p})^s} + S(\alpha), \\ S(\alpha) &= \tfrac{1}{2}\sum_{(\mathfrak{p})} \left\{\frac{\alpha}{\mathfrak{p}}\right\}^2 \frac{1}{n(\mathfrak{p})^{2s}} + \tfrac{1}{3}\sum_{(\mathfrak{p})} \left\{\frac{\alpha}{\mathfrak{p}}\right\}^3 \frac{1}{n(\mathfrak{p})^{3s}} + \cdots\end{aligned}\right\} \quad (30.3)$$

and here also $S(\alpha)$ remains finite for $s = 1$. Let now m be one of the numbers $1, 2, \ldots, l-1$; then in (30.3) we set

$$\alpha = \alpha_*^m = \alpha_1^{mu_1} \alpha_2^{mu_2} \cdots \alpha_t^{mu_t}$$

and multiply the resulting equation by the factor $\gamma_1^{-u_1}\gamma_2^{-u_2}\cdots\gamma_t^{-u_t}$. We give each of the t exponents $u_1, u_2, \ldots, u_t$ successively all l values $0, 1, \ldots, l-1$, excluding the case where $u_1 = u_2 = \ldots = u_t = 0$. When we add to (30.2) all the $l^t - 1$ equations produced in this way we obtain the relation

$$\left.\begin{aligned}&\sum_{(\mathfrak{p})} \frac{1}{n(\mathfrak{p})^s} + S + \\ &\qquad \sum_{(u_1,\ldots,u_t)} \gamma_1^{-u_1}\cdots\gamma_t^{-u_t} \log \prod_{(\mathfrak{p})} \frac{1}{1-\left\{\frac{\alpha_1^{u_1}\cdots\alpha_t^{u_t}}{\mathfrak{p}}\right\}^m n(\mathfrak{p})^{-s}} \\ &= \sum_{(\mathfrak{p})} [1][2]\cdots[t] \frac{1}{n(\mathfrak{p})^s} + S + \sum_{(u_1,\ldots,u_t)} \gamma_1^{-u_1}\cdots\gamma_t^{-u_t} S(\alpha_*^m)\end{aligned}\right\} \quad (30.4)$$

where we write for a moment

$$\begin{aligned}
[1] &= 1+(\gamma_1^{-1}\left\{\frac{\alpha_1}{\mathfrak{p}}\right\}^m)+(\gamma_1^{-1}\left\{\frac{\alpha_1}{\mathfrak{p}}\right\}^m)^2+\cdots+(\gamma_1^{-1}\left\{\frac{\alpha_1}{\mathfrak{p}}\right\}^m)^{l-1},\\
[2] &= 1+(\gamma_2^{-1}\left\{\frac{\alpha_2}{\mathfrak{p}}\right\}^m)+(\gamma_2^{-1}\left\{\frac{\alpha_2}{\mathfrak{p}}\right\}^m)^2+\cdots+(\gamma_2^{-1}\left\{\frac{\alpha_2}{\mathfrak{p}}\right\}^m)^{l-1},\\
&\cdots\cdots\cdots\\
[t] &= 1+(\gamma_t^{-1}\left\{\frac{\alpha_t}{\mathfrak{p}}\right\}^m)+(\gamma_t^{-1}\left\{\frac{\alpha_t}{\mathfrak{p}}\right\}^m)^2+\cdots+(\gamma_t^{-1}\left\{\frac{\alpha_t}{\mathfrak{p}}\right\}^m)^{l-1}.
\end{aligned}$$

In $S(\alpha_*^m)$ we set the above expression for α_*^m.

There are only finitely many prime ideals $\mathfrak{p}$ dividing $\alpha_1, \ldots, \alpha_t, \lambda$; let the sum of the terms in the first sum on the right hand side of (30.4) which correspond to these ideals $\mathfrak{p}$ be denoted by G_m. The remaining, infinite, part of this sum clearly has the value $l^t \sum\limits_{\mathfrak{q}} \frac{1}{n(\mathfrak{q})^s}$ where $\mathfrak{q}$ runs through only those prime ideals $\mathfrak{p}$ for which the t conditions

$$\left\{\frac{\alpha_1}{\mathfrak{p}}\right\}^m = \gamma_1, \ldots, \left\{\frac{\alpha_t}{\mathfrak{p}}\right\}^m = \gamma_t \tag{30.5}$$

are all fulfilled. We now form the equations (30.4) for $m = 1, 2, \ldots, l-1$ successively and add the results, obtaining

$$\left.\begin{aligned}
&(l-1)\sum_{(\mathfrak{p})}\frac{1}{n(\mathfrak{p})^s}+(l-1)S\\
&+\sum_{(u_1,\ldots,u_t)}\gamma_1^{-u_1}\cdots\gamma_t^{-u_t}\log\prod_{(\mathfrak{p})}\prod_{(m)}\frac{1}{1-\left\{\frac{\alpha_1^{u_1}\cdots\alpha_t^{u_t}}{\mathfrak{p}}\right\}n(\mathfrak{p})^{-s}}\\
&\qquad=l^t\sum_{(\mathfrak{r})}\frac{1}{n(\mathfrak{r})^s}+\sum_{(m)}G_m+(l-1)S+\\
&\qquad\sum_{(u_1,\ldots,u_t)}\gamma_1^{-u_1}\cdots\gamma_t^{-u_t}\sum_{(m)}S(\alpha_*^m);
\end{aligned}\right\} \tag{30.6}$$

in the first sum on the right hand side $\mathfrak{r}$ runs through all prime ideals $\mathfrak{p}$ of $k(\zeta)$ which satisfy any one of the sets of conditions (30.5) as we take $m = 1, 2, \ldots, l-1$. (For $\gamma_1 = 1, \ldots, \gamma_t = 1$ these sets of conditions are all the same and the corresponding prime ideals are to be counted $l-1$ times.) Now we take the limit at $s = 1$. According to the arguments at the beginning of the proof the first sum $\sum$ on the left hand side of (30.6) increases beyond bound; from Lemma 27 we see that the second sum on the left remains finite for $s = 1$. Since the sums S and $S(\alpha_*^m)$ all remain finite for $s = 1$ it follows that the sum $\sum\limits_{(\mathfrak{r})}\frac{1}{n(\mathfrak{r})^s}$ increases beyond bounds as s approaches 1. Hence there must be infinitely many terms of the sum $\sum\limits_{(\mathfrak{r})}$ and hence infinitely many prime ideals $\mathfrak{r}$ whose power characters satisfy the conditions of Theorem 152.

31. Regular Cyclotomic Fields

§136. Definition of Regular Cyclotomic Fields, Regular Prime Numbers and Regular Kummer Fields

Let l be an odd prime number and $k(\zeta)$ the cyclotomic field generated by $\zeta = e^{2\pi i/l}$; $k(\zeta)$ is called a *regular cyclotomic field* and l is called a *regular prime number* if the number of ideal classes of the field $k(\zeta)$ is not divisible by l. The remaining chapters will be concerned exclusively with regular cyclotomic fields and with Kummer fields derived from them. Such Kummer fields will be called *regular Kummer fields.* We can prove at once the following simple result.

Theorem 153. *Let $k(\zeta)$ be a regular cyclotomic field, K a Kummer field derived from it. If an ideal $\mathfrak{i}$ of $k(\zeta)$ is a principal ideal in K then it is also a principal ideal in the cyclotomic field $k(\zeta)$ itself.*

Proof. Suppose $\mathfrak{i} = (\mathsf{A})$ where A is an integer in K. Then, taking relative norms, we have $\mathfrak{i}^l = (N_k(\mathsf{A}))$; so we have the equivalence $\mathfrak{i}^l \sim 1$ in $k(\zeta)$. Of course we have also $\mathfrak{i}^h \sim 1$ where h is the class number of $k(\zeta)$. We determine two positive rational integers a and b such that $al - bh = 1$; it follows that $\mathfrak{i}^{al-bh} \sim 1$, i.e. that $\mathfrak{i}$ is a principal ideal in $k(\zeta)$.

The question now arises whether we can find a criterion by which we can decide easily whether a given prime number l is regular. We shall prove two lemmas which lead to such a criterion.

§137. A Lemma on the Divisibility by l of the First Factor of the Class Number of $k(e^{2\pi i/l})$

Lemma 28. *Let l be an odd prime number and $k(\zeta)$ the cyclotomic field of the l-th roots of unity. The first factor of the class number of $k(\zeta)$ is divisible by l if and only if l divides the numerator of one of the first $l^* = \frac{1}{2}(l-3)$ Bernoulli numbers (Kummer (8), Kronecker (5)).*

Proof. In Theorem 142 the class number h was represented as the product of two factors; we consider the expression given there for the first factor of the class number. For brevity we shall write $\mathsf{Z} = e^{2\pi i/(l-1)}$. We shall choose the primitive root r modulo l so that $r^{\frac{1}{2}(l-1)} + 1$ is divisible by only the first power of l. Finally, as in Sect. 108 and Sect. 109, let r_i be the least positive residue of r^i modulo l and $q_i = (rr_i - r_{i+1})/l$.

The first factor of the class number h was represented in Theorem 142 as a fraction whose denominator is $(2l)^{l^*}$ and whose numerator has the form

$$f(\mathsf{Z})f(\mathsf{Z}^3)f(\mathsf{Z}^5)\cdots f(\mathsf{Z}^{l-2}) \tag{31.1}$$

where $f(x)$ is an abbreviation for the integer polynomial

$$f(x) = r_0 + r_1 x + r_2 x^2 + \cdots + r_{l-2} x^{l-2}.$$

If we set

$$g(x) = q_0 + q_1 x + q_2 x^2 + \cdots + q_{l-2} x^{l-2}$$

then it follows easily that

$$(r\mathsf{Z} - 1) f(\mathsf{Z}) = l\mathsf{Z} \cdot g(\mathsf{Z}).$$

From the choice of r we see that the product

$$(r\mathsf{Z} - 1)(r\mathsf{Z}^3 - 1)\cdots(r\mathsf{Z}^{l-2} - 1) = (-1)^{\frac{1}{2}(l-1)}(r^{\frac{1}{2}(l-1)} + 1)$$

is divisible by precisely the first power of l. It follows that the numerator (31.1) of the first factor of h is divisible by $l^{\frac{1}{2}(l-1)} = l^{l^*+1}$ only if the number

$$g(\mathsf{Z})g(\mathsf{Z}^3)g(\mathsf{Z}^5)\cdots g(\mathsf{Z}^{l-2})$$

is divisible by l. Now $\mathfrak{L} = (l, \mathsf{Z} - r)$ is a prime ideal of $k(\zeta)$ dividing l; since clearly $\mathsf{Z} \equiv r \pmod{\mathfrak{L}}$ we have

$$g(\mathsf{Z})g(\mathsf{Z}^3)g(\mathsf{Z}^5)\cdots g(\mathsf{Z}^{l-2}) \equiv g(r)g(r^3)g(r^5)\cdots g(r^{l-2}) \pmod{\mathfrak{L}}.$$

Thus the first factor of the class number h is divisible by l only if at least one of the congruences

$$g(r^{2t-1}) = q_0 + q_1 r^{2t-1} + q_2 r^{2(2t-1)} + \cdots + q_{l-2} r^{(l-2)(2t-1)} \equiv 0 \pmod{l}$$
$$(t = 1, 2, 3, \ldots, \tfrac{1}{2}(l-1))$$

is satisfied.

Let t be one of the numbers $1, 2, 3, \ldots, \frac{1}{2}(l-1)$. If we raise the identity

$$rr_i = r_{i+1} + (rr_i - r_{i+1})$$

to the $(2t)$-th power and recall that $rr_i - r_{i+1}$ is divisible by l then we obtain the congruence

$$r^{2t} r_i^{2t} \equiv r_{i+1}^{2t} + 2t(rr_i - r_{i+1}) r_{i+1}^{2t-1} \pmod{l^2}$$

or

$$2t(rr_i - r_{i+1})r_{i+1}^{2t-1} \equiv r^{2t}r_i^{2t} - r_{i+1}^{2t} \pmod{l^2}.$$

Since obviously

$$(rr_i - r_{i+1})r_{i+1}^{2t-1} \equiv (rr_i - r_{i+1})r^{(i+1)(2t-1)} \pmod{l^2}$$

it follows that

$$2t(rr_i - r_{i+1})r^{(i+1)(2t-1)} \equiv r^{2t}r_i^{2t} - r_{i+1}^{2t} \pmod{l^2}.$$

Summing these congruences for $i = 0, 1, 2, \ldots, l-2$, we obtain

$$2tlr^{2t-1}\sum_{(i)} q_i r^{i(2t-1)} \equiv r^{2t}\sum_{(i)} r_i^{2t} - \sum_{(i)} r_{i+1}^{2t}. \pmod{l^2}.$$

Since we have

$$\sum_{(i)} r_i^{2t} = \sum_{(i)} r_{i+1}^{2t} = 1^{2t} + 2^{2t} + 3^{2t} + \cdots + (l-1)^{2t}$$

it follows that $g(r^{2t-1})$ is divisible by l if and only if the number

$$(r^{2t} - 1)(1^{2t} + 2^{2t} + 3^{2t} + \cdots + (l-1)^{2t}) \tag{31.2}$$

is divisible by l^2. According to the hypothesis made concerning the primitive root r the expression (31.2) is certainly not divisible by l^2 when $t = \frac{1}{2}(l-1)$. It follows from the Bernoulli summation formula that in each case

$$1^{2t} + 2^{2t} + 3^{2t} + \cdots + (l-1)^{2t} \equiv (-1)^{t+1}B_t l \pmod{l^2}$$

where B_t is the t-th *Bernoulli number* ($t = 1, 2, \ldots, \frac{1}{2}(l-3)$). Thus we see that the divisibility by l^2 of at least one of the numbers (31.2) for $t = 1, 2, \ldots, \frac{1}{2}(l-3)$ is equivalent to the divisibility by l of the numerator of at least one of the first $\frac{1}{2}(l-3)$ Bernoulli numbers.

This completes the proof of Lemma 28.

§138. A Lemma on the Units of the Cyclotomic Field $k(e^{2\pi i/l})$ When l Does Not Divide the Numerators of the First $\frac{1}{2}(l-3)$ Bernoulli Numbers

Lemma 29. *Let l be an odd prime number which does not divide the numerators of the first $l^* = \frac{1}{2}(l-3)$ Bernoulli numbers. Then by forming appropriate products and quotients of the cyclotomic units of the field $k(\zeta)$ of the l-th roots of unity we can construct a set of l^* units $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{l^*}$ which satisfy l^* congruences of the form*

$$\left.\begin{array}{lcll} \varepsilon_1 & \equiv & 1+a_1\lambda^2 & (\mathrm{mod}\ \mathfrak{l}^3) \\ \varepsilon_2 & \equiv & 1+a_2\lambda^4 & (\mathrm{mod}\ \mathfrak{l}^5) \\ \varepsilon_3 & \equiv & 1+a_3\lambda^6 & (\mathrm{mod}\ \mathfrak{l}^7) \\ & & \cdots\cdots\cdots & \\ \varepsilon_{l^*} & \equiv & 1+a_{l^*}\lambda^{l-3} & (\mathrm{mod}\ \mathfrak{l}^{l-2}) \end{array}\right\} \tag{31.3}$$

where $a_1, a_2, \ldots, a_{l^*}$ *are rational integers not divisible by* l, $\lambda = 1-\zeta$ *and* $\mathfrak{l} = (\lambda)$ (*Kummer* (12)).

Proof. We start from the cyclotomic unit

$$\varepsilon = \sqrt{\frac{(1-\zeta^r)(1-\zeta^{-r})}{(1-\zeta)(1-\zeta^{-1})}}, \tag{31.4}$$

where r is a primitive root modulo l. (See Sect. 98.) Then we set $\eta = \varepsilon^{l-1}$ and

$$\varepsilon_t = \eta^{(r^2-s)(r^4-s)(r^6-s)\cdots(r^{2t-2}-s)(r^{2t+2}-s)(r^{2t+4}-s)\cdots(r^{l-3}-s)} \tag{31.5}$$

for $t = 1, 2, 3, \ldots, l^*$. This is to be understood as a symbolic power with $s = (\zeta : \zeta^r)$.

Since η is the $(l-1)$-st power of an integer in $k(\zeta)$ we must have $\eta \equiv 1$ (mod $\mathfrak{l}$), and the same holds also for each of the units ε_t. For each index t we consider the function $\varepsilon_t(x)$ belonging to the unit ε_t according to Sect. 131. Then we shall show that the rational numbers

$$\mathrm{l}^{(1)}(\varepsilon_t), \mathrm{l}^{(2)}(\varepsilon_t), \ldots, \mathrm{l}^{(l-2)}(\varepsilon_t),$$

i.e. the values of the first $l-2$ derivatives of the logarithm of $\varepsilon_t(e^v)$ at the place $v = 0$, satisfy the congruences

$$\left.\begin{array}{l} \mathrm{l}^{(u)}(\varepsilon_t) \equiv 0 \pmod{l} \\ \qquad (u = 1, 2, 3, \ldots, 2t-1, 2t+1, \ldots, l-3, l-2) \\ \mathrm{l}^{(2t)}(\varepsilon_t) \equiv (-1)^{t+l^*} \dfrac{B_t}{4tr^{2t}} \pmod{l} \\ \qquad\qquad (t = 1, 2, \ldots, l^*). \end{array}\right\} \tag{31.6}$$

To prove this we notice that according to the formulæ on p.245 for the determination of the first $l-2$ derivatives

$$\mathrm{l}^{(1)}(\eta), \mathrm{l}^{(2)}(\eta), \ldots, \mathrm{l}^{(l-2)}(\eta)$$

with respect to η we may take in place of the function belonging to η the following function

$$\bar{\eta}(x) = \left(\frac{(1-x^r)(1-x^{-r})}{(1-x)(1-x^{-1})}\right)^{\frac{1}{2}(l-1)}$$

We have the well-known expansion

$$\log\frac{e^v-1}{v}=+\frac{1}{2}v+\frac{B_1}{2\cdot 2!}v^2-\frac{B_2}{4\cdot 4!}v^4+\frac{B_3}{6\cdot 6!}v^6-\cdots,$$

where B_1, B_2, B_3, ... are the Bernoulli numbers. From this infinite series we deduce that

$$\left.\begin{aligned}\log(\tilde\eta(e^v))=(l-1)\{&\log r+(r^2-1)\frac{B_1}{2\cdot 2!}v^2\\ &-(r^4-1)\frac{B_2}{4\cdot 4!}v^4+(r^6-1)\frac{B_3}{6\cdot 6!}v^6-\ldots\}.\end{aligned}\right\}\tag{31.7}$$

Just as $\tilde\eta(e^v)$ corresponds to the number η, the function $\tilde\eta(e^{rv})$ corresponds to $s\eta$, the function $\tilde\eta(e^{r^2v})$ to $s^2\eta$ and so on. In the expansion of the expression (31.5) for ε_t we replace η, $s\eta$, $s^2\eta$, ... by $\tilde\eta(e^v)$, $\tilde\eta(e^{rv})$, $\tilde\eta(e^{r^2v})$, ... and so obtain a function $\tilde\varepsilon_t(e^v)$ which can be used in place of $\varepsilon_t(e^v)$ in the procedure on p. 241 for forming $\mathrm{l}^{(1)}(\varepsilon_t)$, $\mathrm{l}^{(2)}(\varepsilon_t)$, ..., $\mathrm{l}^{(l-2)}(\varepsilon_t)$. From (31.7) we have

$$\begin{aligned}\log\tilde\varepsilon_t(e^v)=(l-1)\{&C+(-1)^t(r^2-r^{2t})(r^4-r^{2t})\cdots\\ &\cdots(r^{2t-2}-r^{2t})(r^{2t+2}-r^{2t})(r^{2t+4}-r^{2t})\cdots\\ &\cdots(r^{l-3}-r^{2t})(1-r^{2t})\frac{B_t}{2t(2t)!}v^{2t}\}\\ &+C_{l-1}v^{l-1}+C_{l+1}v^{l+1}+\cdots,\end{aligned}$$

where C, C_{l-1}, C_{l+1}, ... are certain constants. The product shown in detail as the coefficient of v^{2t} is

$$(-1)^{l^*}\left[\frac{d(x-1)(x-r^2)\cdots(x-r^{l-3})}{dx}\right]_{x=r^{2t}}$$

and the function which is differentiated here is congruent to $x^{\frac{1}{2}(l-1)}-1$ modulo l. From this discussion we deduce at once the congruences (31.6).

According to our hypothesis the numerators of the first l^* Bernoulli numbers B_1, ..., B_{l^*} are not divisible by l; so it follows from (31.6) that the l^* derivatives $\mathrm{l}^{(2t)}(\varepsilon_t)$ for $t=1, 2, \ldots, l^*$ are all incongruent to 0 modulo l. From this we conclude that none of the units ε_1, ..., ε_{l^*} is congruent to 1 modulo l. Let us set

$$\left.\begin{aligned}\varepsilon_1 &\equiv 1+a_1\lambda^{e_1} \pmod{\mathfrak{l}^{e_1+1}}\\ &\cdots\cdots\\ \varepsilon_{l^*} &\equiv 1+a_{l^*}\lambda^{e_{l^*}} \pmod{\mathfrak{l}^{e_{l^*}+1}}\end{aligned}\right\}\tag{31.8}$$

where the exponents $e_1, \ldots, e_{l^*}$ are such that $a_1, \ldots, a_{l^*}$ are rational integers not divisible by l. These exponents e_1, ..., e_{l^*} are all less that $l-1$. Now, since the expansion of an expression $(1-e^v)^g$ in powers of v begins with the

term $(-1)^g v^g$, we deduce from the congruences (31.8) that for each unit ε_t we have the congruences

$$1^{(1)}(\varepsilon_t) \equiv 0, 1^{(2)}(\varepsilon_t) \equiv 0, \ldots, 1^{(e_t-1)}(\varepsilon_t) \equiv 0 \pmod{l},$$
$$1^{(e_t)}(\varepsilon_t) \equiv (-1)^{e_t} a_t \cdot e_t! \pmod{l}.$$

Since a_t is not divisible by l it follows, when we take account of the consequences of (31.6) already mentioned, that $e_t = 2t$ and hence Lemma 29 is established.

§139. A Criterion for Regular Prime Numbers

The following theorem gives a simple criterion for the regularity of a prime number l.

Theorem 154. *An odd prime number l is regular if and only if it does not divide the numerators of the first $l^* = \frac{1}{2}(l-3)$ Bernoulli numbers* (*Kummer* (8)).

Proof. Lemma 28 shows that if l divides the numerator of at least one of the first l^* Bernoulli numbers then the class number h of the field $k(\zeta)$ is divisible by l. If, on the other hand, the numerators of the first l^* Bernoulli numbers are all prime to l then Lemma 28 shows also that the first factor of the class number is prime to l. We must therefore show that if the numerators of the first l^* Bernoulli numbers are all prime to l then the second factor of the class number h is also not divisible by l. The proof of this is carried out as follows.

Let $\gamma_1, \ldots, \gamma_{l^*}$ be a fundamental set of l^* real units of the field $k(\zeta)$; such a set exists by Theorem 127. Then we can write

$$s^t\varepsilon = \gamma_1^{m_{1t}}\gamma_2^{m_{2t}}\cdots\gamma_{l^*}^{m_{l^*t}} \tag{31.9}$$

for $t = 0, 1, \ldots, l^*-1$, where ε is the cyclotomic unit defined by the formula (31.4) and $m_{1t}, m_{2t}, \ldots, m_{l^*t}$ are rational integers. From (31.9) we obtain

$$\log|s^t\varepsilon| = m_{1t}\log|\gamma_1| + m_{2t}\log|\gamma_2| + \cdots + m_{l^*t}|\gamma_{l^*}| \tag{31.10}$$

for $t = 0, 1, \ldots, l^*-1$, where we always take the real values of the logarithms. On the other hand the defining equations (31.5) of the units $\varepsilon_1, \ldots, \varepsilon_{l^*}$ give rise to a set of equations of the form

$$\varepsilon_t = \varepsilon^{n_{1t}}(s\varepsilon)^{n_{2t}}\cdots(s^{l^*-1}\varepsilon)^{n_{l^*}} \quad (t = 1, 2, \ldots, l^*) \tag{31.11}$$

from which we have the equations

$$\log\varepsilon_t = n_{1t}\log|\varepsilon| + n_{2t}\log|s\varepsilon| + \cdots + n_{l^*t}\log|s^{l^*-1}\varepsilon| \quad (t = 1, 2, \ldots, l^*) \tag{31.12}$$

where again we take the real values of the logarithms. (31.10) can thus be written

$$\log \varepsilon_t = M_{1t} \log |\gamma_1| + \cdots + M_{l^*t} \log |\gamma_{l^*}| \quad (t = 1, 2, \ldots, l^*) \tag{31.13}$$

where $M_{1t}, \ldots, M_{l^*t}$ are familiar bilinear combinations of the $2(l^*)^2$ rational integers $n_{11}, n_{21}, \ldots, n_{l^*l^*}$; $m_{10}, m_{20}, \ldots, m_{l^*,l^*-1}$. From the equations (31.9) and (31.11) we can deduce $l^* - 1$ further sets of equations by applying the automorphisms $s, s^2, \ldots, s^{l^*-1}$ in succession to the units occurring in them. Taking logarithms we obtain the sets of equations which are derived from (31.10), (31.12) and (31.13) by applying the automorphisms $s, s^2, \ldots, s^{l^*-1}$ in succession to the units occurring in them.

If we set

$$R = \begin{vmatrix} \log|\gamma_1| & \ldots & \log|\gamma_{l^*}| \\ \log|s\gamma_1| & \ldots & \log|s\gamma_{l^*}| \\ & \cdots\cdots & \\ \log|s^{l^*-1}\gamma_1| & \ldots & \log|s^{l^*-1}\gamma_{l^*}| \end{vmatrix},$$

$$\Delta = \begin{vmatrix} \log|\varepsilon| & \log|s\varepsilon| & \ldots & \log|s^{l^*-1}\varepsilon| \\ \log|s\varepsilon| & \log|s^2\varepsilon| & \ldots & \log|s^{l^*}\varepsilon| \\ & & \cdots\cdots & \\ \log|s^{l^*-1}\varepsilon| & \log|s^{l^*}\varepsilon| & \ldots & \log|s^{2l^*-2}\varepsilon| \end{vmatrix},$$

$$\bar{\Delta} = \begin{vmatrix} \log\varepsilon_1 & \log\varepsilon_2 & \ldots & \log\varepsilon_{l^*} \\ \log s\varepsilon_1 & \log s\varepsilon_2 & \ldots & \log s\varepsilon_{l^*} \\ & & \cdots\cdots & \\ \log s^{l^*-1}\varepsilon_1 & \log s^{l^*-1}\varepsilon_2 & \ldots & \log s^{l^*-1}\varepsilon_{l^*} \end{vmatrix},$$

then, by the multiplication theorem for determinants, we have

$$\frac{\bar{\Delta}}{R} = \frac{\bar{\Delta}}{\Delta} \cdot \frac{\Delta}{R} = \begin{vmatrix} M_{11} & M_{21} & \ldots & M_{l^*1} \\ M_{12} & M_{22} & \ldots & M_{l^*2} \\ & & \cdots\cdots & \\ M_{1l^*} & M_{2l^*} & \ldots & M_{l^*l^*} \end{vmatrix}. \tag{31.14}$$

The determinant on the right hand side is a rational integer, which we claim is prime to l. If this determinant were divisible by l we would be able to find l^* rational integers $N_1, \ldots, N_{l^*}$ not all divisible by l for which the expressions

$$\sum_{(t)} N_t M_{1t}, \quad \sum_{(t)} N_t M_{2t}, \quad \ldots, \quad \sum_{(t)} N_t M_{l^*t} \quad (t = 1, 2, \ldots, l^*)$$

are all divisible by l. We would then be able to deduce from (31.13) an equation of the form

$$N_1 \log\varepsilon_1 + N_2 \log\varepsilon_2 + \cdots + N_{l^*} \log\varepsilon_{l^*} = l \log \mathrm{E}$$

in which E is a certain positive unit of the field $k(\zeta)$. Taking the exponential of both sides we have

$$\varepsilon_1^{N_1}\varepsilon_2^{N_2}\cdots\varepsilon_{l^*}^{N_{l^*}} = \mathsf{E}^l. \tag{31.15}$$

But such an equation is impossible. For we would have $\mathsf{E} \equiv \mathsf{E}^l \equiv 1 \pmod{l}$; if we introduce the function $\mathsf{E}(x)$ belonging to E and consider the values of the first $l-2$ derivatives of $\log \mathsf{E}(e^v)$ at $v=0$ then, applying (31.6), we deduce from (31.15) the congruences

$$(-1)^{t+l^*}\frac{B_t}{4tr^{2t}}N_t \equiv 0 \pmod{l} \quad (t = 1, 2, \ldots, l^*).$$

The Bernoulli numbers B_1, B_2, ..., B_{l^*}, however, are all prime to l and the integers N_1, N_2, ..., N_{l^*} are not all divisible by l; so we have a contradiction.

Thus the determinant on the right hand side of (31.14) is not divisible by l. Since the factors $\bar{\Delta}/\Delta$ and Δ/R on the left hand side are both integers and Δ/R is the second factor of the class number h it follows that the second factor of the class number is not divisible by l. This completes the proof of Theorem 154.

Using Theorem 154 we deduce from the values of the first 47 Bernoulli numbers that apart from the three primes 37, 59 and 67 all primes less than 100 are regular. Further calculations show that for $l = 37$, 59 and 67 the class number h of the cyclotomic field $k(e^{2\pi i/l})$ is divisible by the first power of l but by no higher power (*Kummer* (11, 26)).

§140. A Special Independent Set of Units in a Regular Cyclotomic Field

In Sect. 139 we found a way to produce a set of units for a regular cyclotomic field which will be useful in our later development.

Theorem 155. *Let l be a regular prime number. Then the cyclotomic field of the l-th roots of unity has an independent set of $l^* = \frac{1}{2}(l-3)$ units $\bar{\varepsilon}_1$, ..., $\bar{\varepsilon}_{l^*}$ satisfying the congruences*

$$\begin{aligned}
\bar{\varepsilon}_1 &\equiv 1+\lambda^2 \pmod{\mathfrak{l}^3}\\
\bar{\varepsilon}_2 &\equiv 1+\lambda^4 \pmod{\mathfrak{l}^5}\\
&\cdots\cdots\cdots\\
\bar{\varepsilon}_{l^*} &\equiv 1+\lambda^{l-3} \pmod{\mathfrak{l}^{l-2}}
\end{aligned}$$

where $\lambda = 1-\zeta$ and $\mathfrak{l} = (\lambda)$.

Proof. Since the cyclotomic field $k(\zeta)$ is regular it follows from Theorem 154 that the numerators of the first l^* Bernoulli numbers are all prime to l

and consequently, by Lemma 29, there are l^* units $\varepsilon_1, \ldots, \varepsilon_{l^*}$ satisfying the congruences (31.3). Since the coefficients $a_1, \ldots, a_{l^*}$ in these congruences are all prime to l we can find l^* rational integers $b_1, \ldots, b_{l^*}$ such that

$$a_1 b_1 \equiv 1, a_2 b_2 \equiv 1, \ldots, a_{l^*} b_{l^*} \equiv 1 \pmod{l}.$$

If we set

$$\bar{\varepsilon}_1 = \varepsilon_1^{b_1}, \ldots, \bar{\varepsilon}_{l^*} = \varepsilon_{l^*}^{b_{l^*}}$$

these units $\bar{\varepsilon}_1, \ldots, \bar{\varepsilon}_{l^*}$ satisfy the congruences in the statement of Theorem 155.

Furthermore the units $\bar{\varepsilon}_1, \ldots, \bar{\varepsilon}_{l^*}$ form an independent set since the units $\varepsilon_1, \ldots, \varepsilon_{l^*}$ determined in Sect. 138 form such a set. To justify this last statement let us suppose to the contrary that we have an equation of the form

$$\varepsilon_1^{e_1} \cdots \varepsilon_{l^*}^{e_{l^*}} = 1, \tag{31.16}$$

where the exponents $e_1, \ldots, e_{l^*}$ are rational integers not all zero. Then we may make the further assumption that the exponents $e_1, \ldots, e_{l^*}$ are not all divisible by l, for, if they were, we would have

$$\varepsilon_1^{e_1/l} \cdots \varepsilon_{l^*}^{e_{l^*}/l} = 1.$$

But if the exponents $e_1, \ldots, e_{l^*}$ are not all divisible by l then equation (31.16) has the form of equation (31.15) and we have already shown in Sect. 139 that such an equation is impossible.

§141. A Characteristic Property of the Units of a Regular Cyclotomic Field

Theorem 156. *If l is a regular prime number then any unit E of the field $k(\zeta)$ of the l-th roots of unity which is congruent to a rational integer modulo l is the l-th power of a unit of $k(\zeta)$ (Kummer (8)).*

Proof. Let $\bar{\varepsilon}_1, \ldots, \bar{\varepsilon}_{l^*}$ be a set of units determined as in Theorem 155. Since this set is independent there are rational integers $e, e_1, \ldots, e_{l^*}$, not all zero, such that

$$\mathsf{E}^e = \bar{\varepsilon}_1^{e_1} \cdots \bar{\varepsilon}_{l^*}^{e_{l^*}} \tag{31.17}$$

and, as can be shown at once, we may suppose that the exponents $e, e_1, \ldots, e_{l^*}$ are not all divisible by l. If e were divisible by l then equation (31.17) would have the form of equation (31.15) and we have already shown that no such equation holds. If, on the other hand, e is not divisible by l then we have $\mathsf{E}^e \equiv 1 \pmod{l}$ and hence $\mathsf{E} \equiv 1 \pmod{l}$; then we form the logarithmic derivatives of the functions belonging to both sides of equation (31.17). Since $\mathsf{E} \equiv 1 \pmod{l}$ the numbers $\mathrm{l}^{(g)}(\bar{\varepsilon}_1), \ldots, \mathrm{l}^{(g)}(\bar{\varepsilon}_{l^*})$ are all congruent to 0

modulo l for $g < l-1$; so when we take in particular $g = 2, 4, \ldots, 2l^*$ and substitute the values of the numbers $\mathfrak{l}^{(g)}(\bar{\varepsilon}_1), \ldots, \mathfrak{l}^{(g)}(\bar{\varepsilon}_{l^*})$ from (31.16) we obtain successively $e_1 \equiv 0, \ldots, e_{l^*} \equiv 0 \pmod{l}$. Thus $\mathsf{E}^e = \mathsf{H}^l$ where H is a certain unit of the cyclotomic field and e is, by hypothesis, a rational integer not divisible by l. We determine rational integers a and b such that $ae + bl = 1$; it follows that

$$\mathsf{E} = (\mathsf{H}^a \mathsf{E}^b)^l$$

and this completes the proof of Theorem 156.

An essentially different proof of Theorem 156 is based on the following considerations. If E were not the l-th power of a unit in $k(\zeta)$ then the unit $\mathsf{H} = \mathsf{E}^{1-s}$ could not be the l-th power of a unit: this is clear from the fact that $1-s$ and $1+s+\cdots+s^{l-2}$ are polynomials which (in the sense of congruence modulo l) have no common factor. If, however, E is congruent modulo l to a rational integer, we have $\mathsf{H} \equiv 1 \pmod{\mathfrak{l}^l}$ and so it would follow from the second part of the proof of Theorem 148 that the Kummer field $k(\sqrt[l]{\mathsf{H}}, \zeta)$ has relative discriminant 1 with respect to $k(\zeta)$. Since this Kummer field is an abelian extension of $k(\zeta)$ of degree l it would follow from Theorem 94 that the number of ideal classes of the cyclotomic field $k(\zeta)$ is divisible by l; this contradicts the hypothesis that $k(\zeta)$ is a regular cyclotomic field.

§142. Primary Numbers in Regular Cyclotomic Fields

An integer α of the regular cyclotomic field $k(\zeta)$ is said to be *primary* if (1) it is semi-primary (see p.204) and (2) it has the property that its product with its complex conjugate number $s^{\frac{1}{2}(l-1)}\alpha$ is congruent to a rational integer modulo $l = \mathfrak{l}^{l-1}$. A primary number is thus prime to $\mathfrak{l}$ and satisfies the congruences

$$\alpha \equiv a \pmod{\mathfrak{l}^2},$$

$$\alpha \cdot s^{\frac{1}{2}(l-1)}\alpha \equiv b \pmod{\mathfrak{l}^{l-1}},$$

where a and b are rational integers (*Kummer* (12)). We have the following result.

Theorem 157. *In a regular cyclotomic field $k(\zeta)$ each integer α prime to $\mathfrak{l}$ can be transformed into a primary number on multiplication by a suitable unit* (*Kummer* (12)).

Proof. Let $\beta = \alpha \cdot s^{\frac{1}{2}(l-1)}\alpha$; β is obviously a number of the subfield of $k(\zeta)$ of degree $\frac{1}{2}(l-1)$ and hence satisfies a congruence $\beta \equiv a \pmod{\mathfrak{l}^2}$ where a is a rational integer not divisible by l. Let $\bar{\varepsilon}_1, \ldots, \bar{\varepsilon}_{l^*}$ be the l^* units determined in Sect. 140. If we have $\beta \equiv a + a_1\lambda^2 \pmod{\mathfrak{l}^4}$, where a_1 is a rational integer,

we can find a rational integer u_1 such that $2au_1 + a_1 \equiv 0 \pmod{l}$; then we have

$$\beta\bar{\varepsilon}_1^{2u_1} \equiv a \pmod{\mathfrak{l}^4}.$$

If $\beta\bar{\varepsilon}_1^{2u_1} \equiv a + a_2\lambda^4 \pmod{\mathfrak{l}^6}$, where a_2 is again a rational integer, we can find a rational integer u_2 such that $2au_2 + a_2 \equiv 0 \pmod{l}$; then we obtain

$$\beta\bar{\varepsilon}_1^{2u_1}\bar{\varepsilon}_2^{2u_2} \equiv a \pmod{\mathfrak{l}^6}.$$

Proceeding in this way we produce eventually

$$\bar{\varepsilon} = \bar{\varepsilon}_1^{u_1}\bar{\varepsilon}_2^{u_2}\cdots\bar{\varepsilon}_{l^*}^{u_{l^*}},$$

and $\beta\bar{\varepsilon}^2 \equiv a \pmod{\mathfrak{l}^{l-1}}$. If ζ^* is a power of ζ such that $\zeta^*\alpha$ is semiprimary then clearly $\zeta^*\bar{\varepsilon}\alpha$ is a primary number.

Every real primary number is congruent to a rational integer modulo $l = \mathfrak{l}^{l-1}$. It follows easily from Theorem 156 that a primary unit in $k(\zeta)$ is the l-th power of a unit in $k(\zeta)$.

We now discuss briefly a lemma on primary numbers which will be useful to us later.

Lemma 30. *If ν and μ are primary numbers in the regular cyclotomic field $k(\zeta)$ then we have*

$$\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\} = 1.$$

Proof. We may suppose that ν and μ are both congruent to 1 modulo $\mathfrak{l}$; otherwise their $(l-1)$-st powers would certainly satisfy this condition and since $\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\} = \left\{\frac{\nu^{l-1},\mu^{l-1}}{\mathfrak{l}}\right\}$ (see p. 242) we can consider these powers instead of ν and μ themselves. By (29.12) we have

$$\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}\left\{\frac{\nu, s^{\frac{1}{2}(l-1)}\mu}{\mathfrak{l}}\right\} = \left\{\frac{\nu,\mu\cdot s^{\frac{1}{2}(l-1)}\mu}{\mathfrak{l}}\right\}.$$

By hypothesis we have $\mu\cdot s^{\frac{1}{2}(l-1)}\mu \equiv 1 \pmod{\mathfrak{l}^{l-1}}$ and $\nu \equiv 1 \pmod{\mathfrak{l}^2}$. So it follows from the general definition (29.11) of the symbol $\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}$ in Sect. 131 that $\left\{\frac{\nu,\mu\cdot s^{\frac{1}{2}(l-1)}\mu}{\mathfrak{l}}\right\} = 1$ and hence

$$\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}\left\{\frac{\nu, s^{\frac{1}{2}(l-1)}\mu}{\mathfrak{l}}\right\} = 1.$$

We prove similarly that

$$\left\{\frac{\nu, s^{\frac{1}{2}(l-1)}\mu}{\mathfrak{l}}\right\}\left\{\frac{s^{\frac{1}{2}(l-1)}\nu, s^{\frac{1}{2}(l-1)}\mu}{\mathfrak{l}}\right\} = 1.$$

From (29.13) we have further that

$$\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}\left\{\frac{s^{\frac{1}{2}(l-1)}\nu, s^{\frac{1}{2}(l-1)}\mu}{\mathfrak{l}}\right\} = 1.$$

The last three equations taken together show that

$$\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}^2 = 1 \quad \text{and so} \quad \left\{\frac{\nu,\mu}{\mathfrak{l}}\right\} = 1.$$

This completes the proof of Lemma 30.

32. Ambig Ideal Classes and Genera in Regular Kummer Fields

§143. Unit Bundles in Regular Cyclotomic Fields

Let l be a regular odd prime number; let $k(\zeta)$ be the regular cyclotomic field determined by $\zeta = e^{2\pi i/l}$. A set E of units of $k(\zeta)$ which contains the l-th powers of all the units of $k(\zeta)$ and is closed under the formation of products and quotients is called a *unit bundle*[1] of the cyclotomic field $k(\zeta)$. In each unit bundle E we can find a certain number m of units $\varepsilon_1, \ldots, \varepsilon_m$ such that every unit of $k(\zeta)$ can be expressed uniquely in the form

$$\varepsilon_1^{u_1} \cdots \varepsilon_m^{u_m} \xi^l$$

where the exponents $u_1, \ldots, u_m$ run independently through the range 0, 1, $\ldots, l-1$ and ξ is any unit in $k(\zeta)$. A set of units $\varepsilon_1, \ldots, \varepsilon_m$ with this property is called a *basis* of the unit bundle E. It is clear that the units $\varepsilon_1, \ldots, \varepsilon_m$ of a basis of E cannot satisfy a relation of the form

$$\varepsilon_1^{e_1} \cdots \varepsilon_m^{e_m} = \varepsilon^l$$

where $e_1, \ldots, e_m$ are rational integers not all divisible by l and ε is a unit in $k(\zeta)$. It can be easily shown that all bases of a unit bundle must consist of the same number of units. This number m is thus completely determined by the bundle E: we call it the *degree of the unit bundle.*

The unit bundle which consists precisely of the l-th powers of the units in $k(\zeta)$ is the unit bundle with the fewest possible members; its degree is 0. The totality of all units of the field $k(\zeta)$ is a unit bundle. From the fact that, as we showed in Theorem 127, every unit of $k(\zeta)$ is the product of an l-th root of unity and a real unit and our discussion in the proof of Theorem 157 we conclude that the units denoted in Sect. 140 by $\bar{\varepsilon}_1, \ldots, \bar{\varepsilon}_{\frac{1}{2}(l-3)}$ together with the root of unity ζ form a basis for this most extensive unit bundle. Thus the bundle consisting of all the units of $k(\zeta)$ has degree $\frac{1}{2}(l-1)$; it is obviously the only unit bundle of degree $\frac{1}{2}(l-1)$ and furthermore there can be no unit bundle of degree greater than $\frac{1}{2}(l-1)$.

We easily see moreover that the relative norms of all units of a Kummer field $k(\sqrt[l]{\mu}, \zeta)$ formed from $k(\zeta)$ constitute a unit bundle for $k(\zeta)$; finally, the collection of all units of $k(\zeta)$ which are relative norms (whether of units or of fractions in the Kummer field $k(\sqrt[l]{\mu}, \zeta)$) forms a unit bundle.

[1] German *Einheitenschar*

§144. Ambig Ideals and Ambig Ideal Classes of a Regular Kummer Field

Let $k(\zeta)$ be a regular cyclotomic field, μ an integer of $k(\zeta)$ which is not the l-th power of a number in $k(\zeta)$; we denote by K the regular Kummer field $k(\mathsf{M},\zeta)$ generated by $\mathsf{M} = \sqrt[l]{\mu}$ and ζ. We now seek to advance the theory of such fields by means of ideas and methods analogous to those we used in Chapters 17 and 18 for the theory of quadratic fields.

The group of K over $k(\zeta)$ is generated by the substitution $S = (\mathsf{M} : \zeta\mathsf{M})$. According to Sect. 57 an ideal $\mathfrak{A}$ of K is called an *ambig ideal* if it remains unaltered under the action of S, i.e. if $S\mathfrak{A} = \mathfrak{A}$ and, in addition, $\mathfrak{A}$ is divisible by no ideal of $k(\zeta)$ other than 1. According to Theorem 93 the t prime ideals which divide the relative discriminant of K are all ambig and there are no other ambig prime ideals apart from these. If then $\mathfrak{A}$ is any ambig ideal in K we easily conclude from the fact that $S\mathfrak{A} = \mathfrak{A}$ that every prime ideal of K which divides $\mathfrak{A}$ must be ambig (cf. Sect. 73); from this it follows that the number of all ambig ideals in K is l^t.

Let $\mathfrak{C}$ be an ideal in the ideal class C of the Kummer field K; then the ideal class determined by the relative conjugate ideal $S\mathfrak{C}$ will be denoted by SC. The classes $SC, S^2C, \dots, S^{l-1}C$ are called the *relative conjugate classes* of C. If $F(S)$ is any polynomial of degree $l-1$ in S, say

$$F(S) = a + a_1S + a_2S^2 + \cdots + a_{l-1}S^{l-1},$$

where $a, a_1, \dots, a_{l-1}$ are rational integers, then the ideal class given by the expression

$$C^a(SC)^{a_1}(S^2C)^{a_2}\cdots(S^{l-1}C)^{a_{l-1}}$$

will be called the $F(S)$-th *symbolic power* of the class C and denoted by

$$C^{a+a_1S+a_2S^2+\cdots+a_{l-1}S^{l-1}} = C^{F(S)}.$$

Finally, an ideal class A of the Kummer field K is called an *ambig class* if $A = SA$, i.e. if its $(1-S)$-th symbolic power $A^{1-S} = 1$. The l-th power of any ambig class A contains among its ideals certain ideals of $k(\zeta)$. We see this at once when we notice that since $SA = A$ we have

$$A^l = A^{1+S+S^2+\cdots+S^{l-1}}$$

and that the norm of an ideal in K must be an ideal in $k(\zeta)$.

§145. Class Bundles in Regular Kummer Fields

Let us consider a set of ideal classes of a regular Kummer field, closed under the formation of products and quotients, such that the l-th power of each class in the set contains ideals of the field $k(\zeta)$ and containing in particular

all classes which themselves contain ideals of the field $k(\zeta)$. Such a set of classes is called a *class bundle*[2] of the Kummer field. In each class bundle we can find a certain number n of classes $C_1, \dots, C_n$ with the property that every class in the bundle can be expressed uniquely in the form

$$C_1^{u_1} C_2^{u_2} \cdots C_n^{u_n} c$$

where the exponents $u_1, \dots, u_n$ run independently through the range 0, 1, $\dots, l-1$ and c is a class which contains ideals of $k(\zeta)$. We say that the classes $C_1, \dots, C_n$ form a *basis for the class bundle.* It can easily be shown that for every other basis of the class bundle the number n of classes in the basis is the same. This number n is called the *degree* of the class bundle.

In particular, if every class in a bundle contains ideals of the field $k(\zeta)$, then the bundle has degree 0. Next, for example, the totality of all classes of K containing either ambig ideals or products of ambig ideals with ideals in $k(\zeta)$ is a class bundle. Finally the collection of all ambig ideal classes of a regular Kummer field is a class bundle.

§146. Two General Lemmas on Fundamental Sets of Relative Units of a Cyclic Extension of Odd Prime Number Degree

Before continuing the investigation of the preceding sections we derive two lemmas which are related to Theorem 91 in Sect. 55.

Lemma 31. *Let l be an odd prime number, K a cyclic extension field of degree l over a subfield k. Let S be a non-identical automorphism in the group of K over k. Let $\mathsf{H}_1, \dots, \mathsf{H}_{r+1}$ be a fundamental set of relative units of K with respect to k. Then every unit E of K satisfies an equation of the form*

$$\mathsf{E}^f = \mathsf{H}_1^{F_1(S)} \cdots \mathsf{H}_{r+1}^{F_{r+1}(S)} [\varepsilon],$$

where f is a rational integral exponent not divisible by l, $F_1(S), \dots, F_{r+1}(S)$ are integer polynomials of degree $l-2$ in S and $[\varepsilon]$ is a unit whose l-th power lies in k.

Proof. It follows from the proof of Theorem 91 that the units

$$\mathsf{H}_1, \dots, \mathsf{H}_{r+1}, S\mathsf{H}_1, \dots, S\mathsf{H}_{r+1}, \dots, S^{l-2}\mathsf{H}_1, \dots, S^{l-2}\mathsf{H}_{r+1},$$

together with r fundamental units of the field k form an independent set. Since there are $l(r+1)-1$ units in this set, it follows that if E is any unit of K then there are relations of the form

[2] German *Klassenschar*

$$\mathsf{E}^{G(S)} = \mathsf{H}_1^{G_1(S)} \cdots \mathsf{H}_{r+1}^{G_{r+1}(S)}[\varepsilon], \tag{32.1}$$

where $G(S)$, $G_1(S)$, ..., $G_{r+1}(S)$ are integer polynomials of degree $l-2$ in S, of which the first does not vanish identically and $[\varepsilon]$ is a unit in K such that $[\varepsilon]^l$ lies in k. Among the infinitely many relations of this kind we choose one for which the polynomial $G(\zeta)$ is divisible by the lowest power of $1-\zeta$. We suppose that the relation (32.1) itself satisfies this condition.

We first examine the possibility that $G(\zeta)$ is divisible at least once by $1-\zeta$. By the definition of a fundamental set of relative units in Sect. 55 we must have

$$G_1(\zeta), \ldots, G_{r+1}(\zeta)$$

all divisible by $1-\zeta$. If we raise the equation (32.1) to the $(1-S^2)(1-S^3)\cdots(1-S^{l-1})$-th symbolic power and set

$$G(\zeta) = (1-\zeta)G^*(\zeta),$$

$$G_1(\zeta) = (1-\zeta)G_1^*(\zeta), \ldots, G_{r+1}(\zeta) = (1-\zeta)G_{r+1}^*(\zeta),$$

it follows easily, when we recall that the $(1+S+S^2+\cdots+S^{l-1})$-th symbolic power of a unit in K is a unit in k, that

$$\mathsf{E}^{lG_1^*(S)} = \mathsf{H}_1^{lG_1^*(S)} \cdots \mathsf{H}_{r+1}^{lG_{r+1}^*(S)}[\varepsilon], \tag{32.2}$$

where $[\varepsilon]$ is either a unit in k or the l-th root of a unit in k. According to equation (32.2) the l-th root of this number $[\varepsilon]$ is a number in K and so, as we see easily, is a unit of K whose l-th power lies in k, which we shall again denote by $[\varepsilon]$. Thus we conclude from (32.2) that

$$\mathsf{E}^{G_1^*(S)} = \mathsf{H}_1^{G_1^*(S)} \cdots \mathsf{H}_{r+1}^{G_{r+1}^*(S)}[\varepsilon],$$

where $[\varepsilon]$ is again a unit of K whose l-th power lies in k. This equation has the same form as (32.1), the only difference being that $G^*(\zeta)$ is divisible by a power of $1-\zeta$ one less that $G(\zeta)$. In this way we establish a contradiction to our hypothesis that (32.1) is already a relation in which $G(\zeta)$ is divisible by the lowest possible power of $1-\zeta$. It follows then that, under this hypothesis on (32.1), $G(\zeta)$ cannot be divisible by $1-\zeta$.

We now set

$$f = G(\zeta)G(\zeta^2)\cdots G(\zeta^{l-1});$$

f is a rational integer not divisible by l and we can find two integer polynomials $H(S)$, $M(S)$ such that

$$f = H(S)G(S) + M(S)(1+S+S^2+\cdots+S^{l-1})$$

holds identically in S. If we raise the equation (32.1) to the $H(S)$-th symbolic power we obtain a relation with the property described in Lemma 31.

Lemma 32. *With the notation of Lemma 31 let the relative norms of the $r+1$ fundamental relative units of the cyclic extension K be*

$$\eta_1 = N_k(\mathsf{H}_1), \ldots, \eta_{r+1} = N_k(\mathsf{H}_{k+1}).$$

Then every unit ε in k which is the relative norm of a unit E in K can be expressed in the form

$$\varepsilon = \eta_1^{u_1} \cdots \eta_{r+1}^{u_{r+1}} [\varepsilon]^l$$

where $u_1, \ldots, u_{r+1}$ are rational integer exponents and $[\varepsilon]$ is a unit in K.

Proof. According to Lemma 31 we have an equation for E of the form

$$\mathsf{E}^f = \mathsf{H}_1^{F_1(S)} \cdots \mathsf{H}_{r+1}^{F_{r+1}(S)} [\varepsilon]$$

(using the notation of Lemma 31). Taking the relative norms of both sides of this equation with respect to k we obtain

$$\varepsilon^f = \eta_1^{F_1(1)} \cdots \eta_{r+1}^{F_{r+1}(1)} [\varepsilon]^l. \tag{32.3}$$

We determine rational integers a and b such that

$$1 = af + bl.$$

Then, raising equation (32.3) to the a-th power, we obtain an equation of the type called for in Lemma 32.

§147. Ideal Classes Determined by Ambig Ideals

Let $K = k(\sqrt[l]{\mu}, \zeta)$ be a regular Kummer field; let S be the substitution $(\sqrt[l]{\mu} : \zeta\sqrt[l]{\mu})$ in the group of K over k. Since an ambig ideal $\mathfrak{A}$ of the field K, by virtue of its property $S\mathfrak{A} = \mathfrak{A}$, determines an ambig ideal class, it follows that to obtain information about the ambig classes we should first study the class bundle derived from the ambig ideals. We prove the following important result.

Theorem 158. *Let t be the number of distinct prime ideals which divide the relative discriminant of the regular Kummer field $K = k(\sqrt[l]{\mu}, \zeta)$ of relative degree l. Suppose the relative norms of all units of K with respect to $k(\zeta)$ form a unit bundle of degree m. Then the classes which contain either ambig ideals of the field K or products of ambig ideals of K with ideals of $k(\zeta)$ form a class bundle of degree*

$$t + m - \tfrac{1}{2}(l+1).$$

Proof. In what follows we assume first of all that the number μ is not of the form $\varepsilon\alpha^l$ where ε is a unit of $k(\zeta)$ and α is a number in $k(\zeta)$. Then every unit $[\varepsilon]$ of the field $K = k(\sqrt[l]{\mu}, \zeta)$ whose l-th power lies in $k(\zeta)$ must itself lie in $k(\zeta)$. Henceforth let $\mathsf{H}_1, \ldots, \mathsf{H}_{\frac{1}{2}(l-1)}$ be a fundamental set of relative units of K with respect to $k(\zeta)$ and let

$$\eta_1 = N_k(\mathsf{H}_1), \ldots, \eta_{\frac{1}{2}(l-1)} = N_k(\mathsf{H}_{\frac{1}{2}(l-1)})$$

be their relative norms.

(1) We consider first the extreme case in which we have $m = \frac{1}{2}(l-1)$. Here we conclude from Lemma 32 that the units $\eta_1, \ldots, \eta_{\frac{1}{2}(l-1)}$ form a basis for the unit bundle consisting of the relative norms of all the units of K. Next we consider the t ambig prime ideals $\mathfrak{L}_1, \ldots, \mathfrak{L}_t$ of K; these determine t ambig ideal classes, which we denote by $L_1, \ldots, L_t$ respectively. In order to determine the degree of the class bundle arising from these classes we set

$$\mathsf{M} = \sqrt[l]{\mu} = \mathfrak{i}\mathfrak{L}_1^{a_1} \cdots \mathfrak{L}_t^{a_t} \tag{32.4}$$

where $a_1, \ldots, a_t$ are rational integer exponents and $\mathfrak{i}$ is an ideal in $k(\zeta)$. According to the hypothesis concerning μ which we made at the beginning, at least one of the exponents $a_1, \ldots, a_t$ must be prime to l; say a_t is not divisible by l. We see from equation (32.4) that

$$c = L_1^{a_1} \cdots L_t^{a_t}$$

is a class containing ideals of $k(\zeta)$. Since L_t^l is also such a class it follows at once that the class L_t can be represented as a product of powers of the classes $L_1, \ldots, L_{t-1}$ and a class containing ideals of the field $k(\zeta)$.

We prove next that no class of the form

$$c' = L_1^{a'_1} \cdots L_{t-1}^{a'_{t-1}} \tag{32.5}$$

formed from the ideal classes $L_1, \ldots, L_{t-1}$ alone, where $a'_1, \ldots, a'_{t-1}$ are rational integer exponents not divisible by l, can contain ideals of $k(\zeta)$. If this were possible then from the relation (32.5) we would be able to set up an equation

$$\mathsf{M}' = \mathfrak{i}'\mathfrak{L}_1^{a'_1} \cdots \mathfrak{L}_{t-1}^{a'_{t-1}} \tag{32.6}$$

with $\mathfrak{i}'$ an ideal of $k(\zeta)$ and M' an integer of the field K. From this we could deduce that $\mathsf{E} = (\mathsf{M}')^{1-S}$ must be a unit in K. Applying Lemma 31 to this unit E we would obtain an equation of the form

$$\mathsf{E}^f = \mathsf{H}_1^{F_1(S)} \cdots H_{\frac{1}{2}(l-1)}^{F_{\frac{1}{2}(l-1)}(S)} \varepsilon \tag{32.7}$$

where f is a rational integer not divisible by l, $F_1(S), \ldots, F_{\frac{1}{2}(l-1)}(S)$ are integer polynomials in S and ε is a unit in $k(\zeta)$. Since we obviously have

$N_k(\mathsf{E}) = 1$ it would follow, on forming relative norms of both sides of (32.7), that

$$1 = \eta_1^{F_1(1)} \cdots \mathsf{H}_{\frac{1}{2}(l-1)}^{F_{\frac{1}{2}(l-1)}(1)} \varepsilon^l.$$

Since $\eta_1, \ldots, \eta_{\frac{1}{2}(l-1)}$ form the basis of a unit bundle the rational integers $F_1(1), \ldots, F_{\frac{1}{2}(l-1)}(1)$ must all be divisible by l and consequently the integers $F_1(\zeta), \ldots, F_{\frac{1}{2}(l-1)}(\zeta)$ must all be divisible by $1 - \zeta$. Let us write

$$F_1(\zeta) = (1-\zeta)F_1^*(\zeta), \ldots, F_{\frac{1}{2}(l-1)}(\zeta) = (1-\zeta)F_{\frac{1}{2}(l-1)}^*(\zeta)$$

and

$$\mathsf{H} = \mathsf{H}_1^{F_1^*(S)} \cdots \mathsf{H}_{\frac{1}{2}(l-1)}^{F_{\frac{1}{2}(l-1)}^*(S)}.$$

Then we have

$$\mathsf{E}^f = \mathsf{H}^{1-S}\varepsilon^*$$

where ε^* is again a unit in $k(\zeta)$. Taking relative norms of both sides of this equation we deduce that

$$1 = (\varepsilon^*)^l,$$

whence $\varepsilon*$ is an l-th root of unity, say $\varepsilon^* = \zeta^g$. Recalling that $\mathsf{M}^{1-S} = \zeta^{-1}$ we have

$$\{(\mathsf{M}')^f \mathsf{M}^g \mathsf{H}^{-1}\}^{1-S} = 1,$$

so that $(\mathsf{M}')^f \mathsf{M}^g \mathsf{H}^{-1}$ is a number in $k(\zeta)$. Now since, according to (32.6), M' is either not divisible by $\mathfrak{L}_t$ or is divisible by $\mathfrak{L}_t$ raised to a power with exponent divisible by l the number M, on the other hand, is divisible by $\mathfrak{L}_t$ raised to a power whose exponent a_t is not divisible by l. So the factorisation of this number into prime ideals of the field $k(\zeta)$ shows first that g must be divisible by l and then, since f is prime to l, that all the exponents $a_1', \ldots, a_{t-1}'$ must be divisible by l. This contradicts our hypothesis. Thus it follows that no relation of the form (32.5) can hold between the classes $L_1, \ldots, L_{t-1}$. So, under the current assumption that $m = \frac{1}{2}(l-1)$, the classes $L_1, \ldots, L_{t-1}$ form a basis for the class bundle derived from the ambig ideals. The degree of this class bundle is therefore $t-1$, which is the result asserted in Theorem 158 when we have $m = \frac{1}{2}(l-1)$.

(2) We suppose secondly that $m = \frac{1}{2}(l-3)$. In this case we must have a relation between the units $\eta_1, \ldots, \eta_{\frac{1}{2}(l-1)}$ of the form $\eta_1^{e_1} \cdots \eta_{\frac{1}{2}(l-1)}^{e_{\frac{1}{2}(l-1)}} = \eta^l$, where the exponents $e_1, \ldots, e_{\frac{1}{2}(l-1)}$ are rational integers not all divisible by l and η is a unit in $k(\zeta)$. If $e_{\frac{1}{2}(l-1)}$, say, is not divisible by l then we may deduce from Lemma 32 that $\eta_1, \ldots, \eta_{\frac{1}{2}(l-3)}$ form a basis for the unit bundle formed by the relative norms of all the units in K. We form the unit

$$\mathsf{E} = \mathsf{H}_1^{e_1} \cdots \mathsf{H}_{\frac{1}{2}(l-1)}^{e_{\frac{1}{2}(l-1)}} \eta^{-1}. \tag{32.8}$$

Since this has relative norm 1 it follows from Theorem 90 (p. 105) that there is an integer Λ in K such that $\mathsf{E} = \Lambda^{1-S}$. We now determine (as is always

possible) a positive rational integer r such that the prime ideal $\mathfrak{L}_t$ occurs as a factor of $\mathsf{M}' = \Lambda\mathsf{M}^r$ raised to a power with exponent divisible by l. Then the prime ideals $\mathfrak{L}_1, \ldots, \mathfrak{L}_{t-1}$ cannot all occur as factors of M' raised to powers with exponents divisible by l; if they did, then, using Theorem 153 (p. 257), we would have $\mathsf{M}' = \Theta\alpha$ with Θ a unit in K and α an integer in $k(\zeta)$. But then it would follow that $\Theta^{1-S} = \mathsf{E}\zeta^{-r}$ and this, having regard to (32.8) and the fact that $e_{\frac{1}{2}(l-1)}$ is prime to l, contradicts the definition of the fundamental set of relative units $\mathsf{H}_1, \ldots, \mathsf{H}_{\frac{1}{2}(l-1)}$ in Sect. 55. Let the ambig prime ideal $\mathfrak{L}_{t-1}$, say, occur as a factor of M' to a power with exponent not divisible by l. We conclude that the class L_{t-1} can be expressed as a product of powers of the classes $L_1, \ldots, L_{t-2}$ and a class containing ideals of $k(\zeta)$.

We prove next that no class

$$c'' = L_1^{a_1''} \cdots L_{t-2}^{a_{t-2}''} \tag{32.9}$$

can be found containing ideals of $k(\zeta)$ where the exponents $a_1'', \ldots, a_{t-2}''$ are rational integers not all divisible by l. If this were the case we could deduce from a relation (32.9) an equation

$$\mathsf{M}'' = \mathfrak{i}''\mathfrak{L}_1^{a_1''} \cdots \mathfrak{L}_{t-2}^{a_{t-2}''} \tag{32.10}$$

where M'' is an integer in K and $\mathfrak{i}''$ is an ideal of $k(\zeta)$. From this we could conclude that $\mathsf{E}' = (\mathsf{M}'')^{1-S}$ must be a unit in K. We apply Lemma 31 to this unit E' and so obtain an equation

$$(\mathsf{E}')^{f'} = \mathsf{H}_1^{F_1'(S)} \cdots \mathsf{H}_{\frac{1}{2}(l-1)}^{F'_{\frac{1}{2}(l-1)}(S)} \varepsilon \tag{32.11}$$

where f' is a rational integer not divisible by l, $F_1'(S), \ldots, F'_{\frac{1}{2}(l-1)}(S)$ are integer polynomials in S and ε is a unit in $k(\zeta)$. We now determine a rational integral exponent u such that the integer $F'_{\frac{1}{2}(l-1)}(1) + ue_{\frac{1}{2}(l-1)}$ is divisible by l. Since $N_k(\mathsf{E}') = 1$ we deduce from (32.11) by taking relative norms with respect to $k(\zeta)$ that

$$1 = \eta_1^{F_1'(1)+ue_1} \cdots \eta_{\frac{1}{2}(l-3)}^{F'_{\frac{1}{2}(l-3)}(1)+ue_{\frac{1}{2}(l-3)}} (\varepsilon')^l \tag{32.12}$$

where ε' is again a unit in $k(\zeta)$. Since the units $\eta_1, \ldots, \eta_{\frac{1}{2}(l-3)}$ form a basis for a unit bundle it follows from (32.12) that the exponents $F_1'(1) + ue_1, \ldots,$ $F'_{\frac{1}{2}(l-3)}(1) + ue_{\frac{1}{2}(l-3)}$ are all divisible by l and so the numbers $F_1'(\zeta) + ue_1,$ $\ldots, F'_{\frac{1}{2}(l-3)}(\zeta) + ue_{\frac{1}{2}(l-3)}$ must all be divisible by $1 - \zeta$. We set

$$F_1'(\zeta) + ue_1 = (1-\zeta)F_1'^*(\zeta), \ldots, F'_{\frac{1}{2}(l-1)}(\zeta) + ue_{\frac{1}{2}(l-1)} = (1-\zeta)F'^*_{\frac{1}{2}(l-1)}(\zeta)$$

and

$$\mathsf{H}' = \mathsf{H}_1^{F_1'^*(S)} \cdots \mathsf{H}_{\frac{1}{2}(l-1)}^{F'^*_{\frac{1}{2}(l-1)}(S)}.$$

Then it follows from (32.11) that

$$(\mathsf{E}')^{f'}\mathsf{E}^u = (\mathsf{H}')^{1-S}\varepsilon'^*$$

where E is the unit of K defined by (32.8) and ε'^* is once more a unit in $k(\zeta)$. Taking relative norms we obtain the result that $1 = (\varepsilon'^*)^l$, i.e. that ε'^* is an l-th root of unity, say $\varepsilon'^* = \zeta^{g'}$. Then, as we see from the equations

$$\mathsf{M}^{1-S} = \zeta^{-1}, (\mathsf{M}')^{1-S} = \mathsf{E}\zeta^{-r}, (\mathsf{M}'')^{1-S} = \mathsf{E}',$$

we have

$$\{(\mathsf{M}'')^{f'}(\mathsf{M}')^u\mathsf{M}^{g-ur}(\mathsf{H}')^{-1}\}^{1-S} = 1.$$

Hence the expression $(\mathsf{M}'')^{f'}(\mathsf{M}')^u\mathsf{M}^{g-ur}(\mathsf{H}')^{-1}$ represents a number in $k(\zeta)$. When we recall that $\mathfrak{L}_t^l, \mathfrak{L}_{t-1}^l, \mathfrak{L}_{t-2}^l, \ldots, \mathfrak{L}_1^l$ are prime ideals in $k(\zeta)$ we conclude first that $g - ur$ must be divisible by l. Then, since (by hypothesis) M' is divisible by a power of $\mathfrak{L}_{t-1}$ with exponent not divisible by l, and since on the other hand it follows from (32.10) that M'' is divisible by a power of $\mathfrak{L}_{t-1}$ with exponent divisible by l, then u also must be divisible by l and hence (since f' is prime to l) the exponents $a_1'', \ldots, a_{t-2}''$ must all be divisible by l – which contradicts our hypothesis concerning these exponents. Thus we have shown that no relation of the form (32.9) can hold between the classes $L_1, \ldots, L_{t-2}$; hence, in the present case where $m = \frac{1}{2}(l-3)$, the classes $L_1, \ldots, L_{t-2}$ form a basis for the class bundle derived from all the ambig ideals. The degree of this class bundle is thus $t-2$ and this corresponds to the assertion of Theorem 158 when $m = \frac{1}{2}(l-3)$.

(3) If we suppose, in the third case, that $m = \frac{1}{2}(l-5)$ then we have not only, as in the previous case, *one* relation between the units $\eta_1, \ldots, \eta_{\frac{1}{2}(l-1)}$ of the form $\eta_1^{e_1}\cdots\eta_{\frac{1}{2}(l-1)}^{e_{\frac{1}{2}(l-1)}} = \eta^l$ where η is a unit in $k(\zeta)$ and the exponents $e_1, \ldots, e_{\frac{1}{2}(l-1)}$ are not all divisible by l but also a *second* relation of the form $\eta_1^{e_1'}\cdots\eta_{\frac{1}{2}(l-3)}^{e'_{\frac{1}{2}(l-3)}} = (\eta')^l$ where η' is a unit in $k(\zeta)$ and the exponents $e_1', \ldots, e'_{\frac{1}{2}(l-3)}$ are not all divisible by l. Say $e_{\frac{1}{2}(l-1)}$ and $e'_{\frac{1}{2}(l-3)}$ are not divisible by l. We form the units

$$\left.\begin{array}{rcl}\mathsf{E} & = & \mathsf{H}_1^{e_1}\cdots\mathsf{H}_{\frac{1}{2}(l-1)}^{e_{\frac{1}{2}(l-1)}}\eta^{-1} \\ \mathsf{E}' & = & \mathsf{H}_1^{e_1'}\cdots\mathsf{H}_{\frac{1}{2}(l-3)}^{e'_{\frac{1}{2}(l-3)}}(\eta')^{-1}.\end{array}\right\} \quad (32.13)$$

Since the units E and E' have relative norms 1 we can apply Theorem 90 (p. 105) and write $\mathsf{E} = \Lambda^{1-S}$ and $\mathsf{E}' = (\Lambda')^{1-S}$ where Λ and Λ' are integers in K. As in the previous case, we then determine a positive rational integer r such that the ideal $\mathfrak{L}_t$ occurs as a factor of $\mathsf{M}' = \Lambda\mathsf{M}^r$ to a power with exponent divisible by l. As in the earlier case it follows that at least one of the ambig prime ideals $\mathfrak{L}_1, \ldots, \mathfrak{L}_{t-1}$ occurs as a factor of M' raised to a

power with exponent not divisible by l; say this is the case for $\mathfrak{L}_{t-1}$. Then we determine two positive rational integers r' and r'' such that the number $\mathsf{M}'' = \Lambda'(\mathsf{M}')^{r'}\mathsf{M}^{r''}$ has as factors powers of $\mathfrak{L}_t$ and $\mathfrak{L}_{t-1}$ with exponents divisible by l. Then $\mathfrak{L}_1, \ldots, \mathfrak{L}_{t-2}$ cannot all occur as factors of M'' raised to powers with exponents divisible by l. For, if this were the case, we could apply Theorem 153 and write $\mathsf{M}'' = \Theta'\alpha'$ where Θ' is a unit of K and α' an integer of $k(\zeta)$. Then, having regard to the equations $\mathsf{M}^{1-S} = \zeta^{-1}$, $\Lambda^{1-S} = \mathsf{E}$, $(\Lambda')^{1-S} = \mathsf{E}'$, we would have

$$(\Theta')^{1-S} = \mathsf{E}'\mathsf{E}^{r'}\zeta^{-(rr'+r'')};$$

according to (32.13) it would follow from this that

$$(\Theta')^{1-S} = \mathsf{H}_1^{e_1'+r'e_1} \cdots \mathsf{H}_{\frac{1}{2}(l-3)}^{e'_{\frac{1}{2}(l-3)}+r'e_{\frac{1}{2}(l-3)}} \mathsf{H}_{\frac{1}{2}(l-1)}^{r'e_{\frac{1}{2}(l-1)}} \varepsilon, \tag{32.14}$$

where ε is a certain unit in $k(\zeta)$. This relation, however, contradicts the definition of a fundamental set of relative units in Sect. 55, for since $e_{\frac{1}{2}(l-1)}$ and $e'_{\frac{1}{2}(l-3)}$ are both prime to l the exponents of $\mathsf{H}_{\frac{1}{2}(l-3)}$ and $\mathsf{H}_{\frac{1}{2}(l-1)}$ in (32.14) can never both be divisible by l. If $\mathfrak{L}_{t-2}$, say, occurs as a factor of M'' to a power with exponent not divisible by l then the ideal class L_{t-2} can be expressed as a product of powers of the classes $L_1, \ldots, L_{t-3}$ and a class containing ideals of $k(\zeta)$.

By arguments similar to those used above in the case where $m = \frac{1}{2}(l-3)$ we can show in the present case where $m = \frac{1}{2}(l-5)$ that there is no class

$$c''' = L_1^{a_1'''} \cdots L_{t-3}^{a_{t-3}'''}$$

containing ideals of $k(\zeta)$, where the exponents $a_1''', \ldots, a_{t-3}'''$ are rational integers not all divisible by l. We now see that in the present case where $m = \frac{1}{2}(l-5)$ the ideal classes $L_1, \ldots, L_{t-3}$ form a basis for the class bundle derived from the ambig ideals. So this bundle has degree $t-3$, which corresponds to the result stated in Theorem 158 for the case where $m = \frac{1}{2}(l-5)$.

By appropriate repetition of the procedure sketched above we obtain finally the complete proof of Theorem 158.

We excluded earlier the case in which the Kummer field K can be generated by a number $\sqrt[l]{\varepsilon}$ where ε is a unit in $k(\zeta)$; so we still have this special case to deal with. According to Theorem 148 the relative discriminant of the field $K = k(\sqrt[l]{\varepsilon}, \zeta)$ can have no prime factor other than $\mathfrak{l}$; by Theorem 94 and Theorem 153 it must actually have $\mathfrak{l}$ as a factor. Then we have in K the factorisation $\mathfrak{l} = \mathfrak{L}^l$ and $\mathfrak{L}$ is the only ambig prime ideal of the field K. Again let $\eta_1, \ldots, \eta_{\frac{1}{2}(l-1)}$ be the relative norms of the fundamental units $\mathsf{H}_1, \ldots, \mathsf{H}_{\frac{1}{2}(l-1)}$ respectively. Since the degree of a unit bundle in $k(\zeta)$ cannot exceed $\frac{1}{2}(l-1)$ there certainly exists a relation of the form

$$\eta_1^{e_1} \cdots \eta_{\frac{1}{2}(l-1)}^{e_{\frac{1}{2}(l-1)}} \varepsilon^{e_{\frac{1}{2}(l+1)}} = \eta^l \tag{32.15}$$

where $e_1, \ldots, e_{\frac{1}{2}(l-1)}, e_{\frac{1}{2}(l+1)}$ are rational integers not all divisible by l and η is a unit in $k(\zeta)$. If we set

$$\mathsf{H} = \mathsf{H}_1^{e_1} \cdots \mathsf{H}_{\frac{1}{2}(l-1)}^{e_{\frac{1}{2}(l-1)}} (\sqrt[l]{\varepsilon})^{e_{\frac{1}{2}(l+1)}} \eta^{-1} \tag{32.16}$$

then we have $N_k(\mathsf{H}) = 1$ and so, by Theorem 90, we have $\mathsf{H} = \Lambda^{1-S}$ where Λ is a suitable integer in K; we can then set $\Lambda = \mathfrak{L}^a \mathfrak{i}$ where $\mathfrak{L}^a$ is a power of the ambig prime ideal $\mathfrak{L}$ and $\mathfrak{i}$ is an ideal in $k(\zeta)$. The exponent a is certainly not divisible by l; for, if it were, then since $\mathfrak{L}^l = \mathfrak{l} = 1 - \zeta$ and taking account of Theorem 153 we would have $\Lambda = \Theta\alpha$ with Θ a unit in K and α a number in $k(\zeta)$. From this, however, we could conclude that $\mathsf{H} = \Theta^{1-S}$ and hence, referring to (32.16), we would have a contradiction to the definition of a fundamental set of relative units in Sect. 55. From the equation $\Lambda = \mathfrak{L}^a\mathfrak{i}$ we see that $\mathfrak{i}^l \sim 1$, whence $\mathfrak{i} \sim 1$ and $\mathfrak{L}^a \sim 1$; since a is prime to l it follows that $\mathfrak{L} \sim 1$. Thus in the case we are at present considering the sole ambig ideal $\mathfrak{L}$ is a principal ideal; thus the degree of the class bundle derived from the ambig ideals is 0.

We now suppose that among the exponents $e_1, \ldots, e_{\frac{1}{2}(l-1)}$ say $e_{\frac{1}{2}(l-1)}$ is prime to l and prove that we can have no relation of the form

$$\eta_1^{e'_1} \cdots \eta_{\frac{1}{2}(l-3)}^{e'_{\frac{1}{2}(l-3)}} \varepsilon^{e'_{\frac{1}{2}(l+1)}} = (\eta')^l \tag{32.17}$$

where $e'_1, \ldots, e'_{\frac{1}{2}(l-3)}, e'_{\frac{1}{2}(l+1)}$ are rational integer exponents not all divisible by l and η' is a unit in $k(\zeta)$. To see this we note that if an equation (32.17) did hold then

$$\mathsf{H}' = \mathsf{H}_1^{e'_1} \cdots \mathsf{H}_{\frac{1}{2}(l-3)}^{e'_{\frac{1}{2}(l-3)}} (\sqrt[l]{\varepsilon})^{e'_{\frac{1}{2}(l+1)}} (\eta')^{-1}$$

would be a unit with relative norm 1. Using Theorem 90 we would have $\mathsf{H}' = (\Lambda')^{1-S}$ where Λ' is a suitable integer in K; then we would determine a positive rational integer exponent r such that the prime ideal $\mathfrak{L}$ occurs as a factor of $\Lambda'\Lambda^r$ raised to a power with exponent divisible by l. Referring to Theorem 153 we set $\Lambda'\Lambda^r = \Theta'\alpha'$ with Θ' a unit in K and α' an integer in $k(\zeta)$; then we would have $(\Theta')^{1-S} = \mathsf{H}'\mathsf{H}^r$, i.e. the unit

$$\mathsf{H}_1^{e'_1+re_1} \cdots \mathsf{H}_{\frac{1}{2}(l-3)}^{e'_{\frac{1}{2}(l-3)}+re_{\frac{1}{2}(l-3)}} \mathsf{H}_{\frac{1}{2}(l-1)}^{re_{\frac{1}{2}(l-1)}} (\sqrt[l]{\varepsilon})^{e'_{\frac{1}{2}(l+1)}+re_{\frac{1}{2}(l+1)}} (\eta')^{-1}\eta^{-r}$$

would be the symbolic $(1-S)$-th power of a unit in K, which leads to a contradiction in a way we have seen several times. Thus we have shown that no relation of the form (32.17) can hold; referring to (32.15) and the fact that $e_{\frac{1}{2}(l-1)}$ is prime to l, we see that the units $\eta_1, \ldots, \eta_{\frac{1}{2}(l-3)}, \varepsilon$ form a basis for the unit bundle formed by the relative norms of all the units in K; hence the degree m of this bundle is $\frac{1}{2}(l-1)$ and so every unit in $k(\zeta)$ is the relative norm of a unit in K. Thus

$$t + m - \tfrac{1}{2}(l+1) = 0$$

and so Theorem 158 is established in this case also.

§148. The Set of All Ambig Ideal Classes

Theorem 158 has revealed a remarkable connexion between the class bundle derived from the ambig ideals and the unit bundle formed by the relative norms of all the units in K. An equally important connexion holds between the class bundle formed by all the ambig classes and a certain unit bundle in $k(\zeta)$. We have the following result.

Theorem 159. *Let t be the number of prime ideals which divide the relative discriminant of a regular Kummer field K of relative degree l. Let the set of all units in $k(\zeta)$ which are relative norms (whether of units or of fractions of the field K) form a unit bundle of degree n. Then the class bundle of all ambig classes has degree $t + n - \frac{1}{2}(l+1)$.*

Proof. Let m have the same meaning as in Theorem 158.

(1) First suppose $n = m$. Then the unit bundle in question here coincides with the unit bundle considered in Theorem 158; that is, if a unit of $k(\zeta)$ is the relative norm of a fraction in K it is also the norm of a unit in K. We shall prove that in this situation the class bundle derived from the ambig ideals is actually the bundle of all ambig classes. To see this, let A be any ambig class in K, $\mathfrak{A}$ an ideal in A; then we can write $\mathfrak{A}^{1-S} = \mathsf{A}$ where A is a suitable integer or fraction in K and the relative norm $N_k(\mathsf{A})$ will obviously be a unit ϑ of the field $k(\zeta)$. As we noted above, in the present case where $n = m$ we can find a unit H of K such that $N_k(\mathsf{H}) = \vartheta$. So we have $N_k(\mathsf{A}^{-1}\mathsf{H}) = 1$ and hence, by Theorem 90, we have $\mathsf{A}^{-1}\mathsf{H} = \mathsf{B}^{1-S}$ or $\mathsf{A}\mathsf{B}^{1-S} = \mathsf{H}$, where B is a suitable integer in K. Since $\mathsf{A} = \mathfrak{A}^{1-S}$ we have $(\mathfrak{A}\mathsf{B})^{1-S} = 1$; thus $\mathfrak{A}\mathsf{B}$ is equal to the product of an ambig ideal and an ideal in $k(\zeta)$. Hence the class A is formed by multiplying a class which contains an ambig ideal and a class which contains ideals of $k(\zeta)$. So our assertion is established and the degree of the class bundle consisting of all ambig classes is, in accordance with Theorem 158, equal to ·

$$t + m - \tfrac{1}{2}(l+1)$$

which, in the present case where $n = m$, is the assertion of Theorem 159.

(2) Secondly let $n = m + 1$. Then there is a unit ϑ in $k(\zeta)$ which is not the relative norm of a unit in K but which is the relative norm of a fraction A in K; further, every other unit ϑ' with this property is expressible in the form $\vartheta' = \vartheta^a \eta$ where a is a rational integer exponent and η is the relative norm of a unit in K. We set

$$\mathsf{A} = \mathfrak{P}_1^{G_1(S)} \cdots \mathfrak{P}_r^{G_r(S)},$$

where $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ are distinct prime ideals of K, no two of which are relative conjugates, and $G_1(S), \dots, G_r(S)$ are integer polynomials of degree $l-1$ in S. Since $N_k(\mathsf{A}) = \vartheta$ we have

$$(\mathfrak{P}_1^{G_1(S)}\cdots\mathfrak{P}_r^{G_r(S)})^{1+S+\cdots+S^{l-1}}=1$$

and from this we deduce easily that the polynomials $G_1(S), \dots, G_r(S)$ must all be divisible by $1-S$. We set

$$G_1(S)=(1-S)G_1^*(S),\dots,G_r(S)=(1-S)G_r^*(S)$$

and

$$\mathfrak{P}_1^{G_1^*(S)}\cdots\mathfrak{P}_r^{G_r^*(S)}=\mathfrak{A}\alpha$$

where $\mathfrak{A}$ is an ideal in K and α is an integer or fraction in $k(\zeta)$; then $\mathsf{A}=\mathfrak{A}^{1-S}$. From this it follows that $\mathfrak{A}$ determines an ambig ideal class, which we denote by A. This class A cannot contain any ideal which is the product of an ambig ideal and an ideal of the field $k(\zeta)$. For, if it did, we could write $\mathfrak{A}=\Gamma\mathfrak{L}\mathfrak{i}$ where Γ is an integer or fraction in K, $\mathfrak{L}$ is an ambig ideal of K and $\mathfrak{i}$ is an ideal of $k(\zeta)$; then, however, we would have $\mathfrak{A}^{1-S}=\Gamma^{1-S}$, whence $\mathsf{A}=\mathsf{H}\Gamma^{1-S}$ where H is a unit in K. From this it would follow that $\vartheta=N_k(\mathsf{A})=N_k(\mathsf{H})$ and this contradicts the defining property of the unit ϑ.

We shall now prove that, under the present assumption that $n=m+1$, every ambig ideal class A' can be expressed in the form $A'=A^aLc$ where A^a is a power of the ideal class A defined above, L is a class containing ambig ideals and c is a class which contains ideals of the field $k(\zeta)$. To this end, let $\mathfrak{A}'$ be any ideal in A'; then we have $(\mathfrak{A}')^{1-S}=\mathsf{A}'$, where A' is a suitable integer or fraction in K. It follows that $\vartheta'=N_k(\mathsf{A}')$ is a unit in $k(\zeta)$; according to our hypothesis on ϑ we have $N_k(\mathsf{A}')=\vartheta^a\eta$, where ϑ, a and η are as described above. Let A be the number introduced above such that $N_k(\mathsf{A})=\vartheta$ and let $\eta=N_k(\mathsf{H})$ where H is a unit in K. From these relations we deduce that $N_k((\mathsf{A}')^{-1}\mathsf{A}^a\mathsf{H})=1$ and hence, by Theorem 90, we have $(\mathsf{A}')^{-1}\mathsf{A}^a\mathsf{H}=\Gamma^{1-S}$ where Γ is an integer in K. From this we deduce that $((\mathfrak{A}')^{-1}\mathfrak{A}^a\Gamma^{-1})^{1-S}=1$. This last equation shows that $(\mathfrak{A}')^{-1}\mathfrak{A}^a\Gamma^{-1}$ on multiplication by a suitable integer of $k(\zeta)$ is the product of an ambig ideal $\mathfrak{L}$ and an ideal $\mathfrak{i}$ of $k(\zeta)$; so we have $\mathfrak{A}'\sim\mathfrak{A}\mathfrak{L}\mathfrak{i}$. In the present case, where $n=m+1$, it follows that the degree of the class bundle consisting of all ambig classes is $t+m+1-\frac{1}{2}(l+1)$, which is the assertion of Theorem 159 in this case.

(3) Thirdly we suppose that $n=m+2$. Then in addition to the unit ϑ there is another unit ϑ' in $k(\zeta)$ which is the relative norm of a fraction A' in K and which cannot be expressed in the form $\vartheta'=\vartheta^a\eta$ where ϑ^a is a power of the unit ϑ introduced above and η is the relative norm of a unit in K. We set

$$\mathsf{A}'=(\mathfrak{P}_1')^{G_1'(S)}\cdots(\mathfrak{P}_{r'}')^{G_{r'}'(S)}$$

where $\mathfrak{P}_1', \dots, \mathfrak{P}_{r'}'$ are prime ideals of K no two of which are equal or relatively conjugate and $G_1'(S), \dots, G_{r'}'(S)$ are integer polynomials of degree $l-1$ in S. Since $N_k(\mathsf{A}')=\vartheta'$ it follows that

$$((\mathfrak{P}_1')^{G_1'(S)}\cdots(\mathfrak{P}_{r'}')^{G_{r'}'(S)})^{1+S+\cdots+S^{l-1}}=1.$$

From this we conclude easily that the polynomials $G'_1(S), \ldots, G'_{r'}(S)$ must all be divisible by $1-S$. If we set

$$G'_1(S) = (1-S)G'^{*}_1(S), \ldots, G'_{r'}(S) = (1-S)G'^{*}_{r'}(S)$$

and

$$(\mathfrak{P}'_1)^{G'^{*}_1(S)} \cdots (\mathfrak{P}'_{r'})^{G'^{*}_{r'}(S)} = \mathfrak{A}'\alpha'$$

where $\mathfrak{A}'$ is an ideal in K and α' an integer or fraction in $k(\zeta)$, then we have $\mathsf{A}' = (\mathfrak{A}')^{1-S}$. Thus the ideal $\mathfrak{A}'$ determines an ambig class A'. This class cannot be expressed in the form $A' = A^a Lc$ where A^a is a power of the class A, L is a class containing an ambig ideal and c is a class containing ideals of $k(\zeta)$. For, if such a representation of A' were possible, we would have $\mathfrak{A}' = \Gamma\mathfrak{A}^a\mathfrak{L}\mathfrak{i}$ where Γ is a number in K, $\mathfrak{L}$ an ambig ideal and $\mathfrak{i}$ an ideal in $k(\zeta)$; but this would imply that $(\mathfrak{A}')^{1-S} = \Gamma^{1-S}\mathfrak{A}^{a(1-S)} = \Gamma^{1-S}\mathsf{A}^a$, i.e. $\mathsf{A}' = \mathsf{H}\Gamma^{1-S}\mathsf{A}^a$ where H is a unit in K. Taking relative norms we have $\vartheta' = N_k(\mathsf{A}') = \vartheta^a N_k(\mathsf{H})$ and the existence of such a relation was ruled out when ϑ' was introduced.

Under the present assumption that $n = m+2$ every unit ϑ'' in $k(\zeta)$ which is the relative norm of a number in K must be expressible in the form $\vartheta'' = (\vartheta')^{a'}\vartheta^a\eta$ where a' and a are rational integer exponents and η is the relative norm of a unit in K. Using this fact we can conclude, by arguments similar to those used above for the case where $n = m+1$, that every ambig class A'' can be represented in the form $(A')^{a'}A^aLc$ where A' and A are the ambig classes introduced above, L is a class containing an ambig ideal and c is a class containing ideals of $k(\zeta)$. From this it follows that the degree of the class bundle consisting of all the ambig classes is precisely $t+m+2-\frac{1}{2}(l+1)$, which is the assertion of Theorem 159 for the case $n = m+2$.

By repetition of this line of argument we obtain the complete proof of Theorem 159.

§149. Character Sets of Numbers and Ideals in Regular Kummer Fields

Our next task is to describe a classification of the ideal classes of a Kummer field $K = k(\sqrt[l]{\mu}, \zeta)$ derived from a regular cyclotomic field corresponding to the classification of the ideal classes of a quadratic field into genera. Suppose there are t distinct prime ideals of $k(\zeta)$ dividing the relative discriminant of K; we denote them by $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$. Corresponding to each nonzero integer ν of $k(\zeta)$ we have t symbols

$$\left\{\frac{\nu,\mu}{\mathfrak{l}_1}\right\}, \ldots, \left\{\frac{\nu,\mu}{\mathfrak{l}_t}\right\}; \tag{32.18}$$

according to the definition in Sect. 131 the values of these symbols are l-th roots of unity. These t roots of unity (32.18) form the *character set* of the

number ν of the Kummer field K. In order to associate a character set also with each ideal $\mathfrak{J}$ of K we form the relative norm $N_k(\mathfrak{J}) = \mathfrak{i}$. We denote by h the number of ideal classes in $k(\zeta)$ and determine a positive rational integer h^* such that $hh^* \equiv 1 \pmod{l}$. Then $\mathfrak{i}^{hh^*}$ is certainly a principal ideal in $k(\zeta)$; we set $\mathfrak{i}^{hh^*} = (\nu)$ where ν is an integer in $k(\zeta)$.

If for every unit ξ_1 of $k(\zeta)$ all t symbols

$$\left\{\frac{\xi_1, \mu}{\mathfrak{l}_1}\right\}, \dots, \left\{\frac{\xi_1, \mu}{\mathfrak{l}_t}\right\}$$

have the value 1 then we set $r = t$ and say that the r roots of unity

$$\left\{\frac{\nu, \mu}{\mathfrak{l}_1}\right\}, \dots, \left\{\frac{\nu, \mu}{\mathfrak{l}_r}\right\}$$

form the *character set* of the ideal $\mathfrak{J}$; the character set is thus completely determined by the ideal $\mathfrak{J}$.

Suppose on the other hand that there exists a particular unit ε_1 in $k(\zeta)$ for which at least one of the t symbols

$$\left\{\frac{\varepsilon_1, \mu}{\mathfrak{l}_1}\right\}, \dots, \left\{\frac{\varepsilon_1, \mu}{\mathfrak{l}_t}\right\}$$

does not take the value 1. Then we may suppose, without loss of generality, that we have $\left\{\frac{\varepsilon_1, \mu}{\mathfrak{l}_t}\right\} = \zeta$. We consider now all the units ξ_2 in $k(\zeta)$ for which $\left\{\frac{\xi_2, \mu}{\mathfrak{l}_t}\right\} = 1$. Suppose that there is among these a unit $\xi_2 = \varepsilon_2$ for which at least one of the $t-1$ symbols

$$\left\{\frac{\varepsilon_2, \mu}{\mathfrak{l}_1}\right\}, \dots, \left\{\frac{\varepsilon_2, \mu}{\mathfrak{l}_{t-1}}\right\}$$

has a value distinct from 1. Then we may suppose that we have, say, $\left\{\frac{\varepsilon_2, \mu}{\mathfrak{l}_{t-1}}\right\} = \zeta$. Now we consider all the units ξ_3 for which both $\left\{\frac{\xi_3, \mu}{\mathfrak{l}_t}\right\} = 1$ and $\left\{\frac{\xi_3, \mu}{\mathfrak{l}_{t-1}}\right\} = 1$ and examine whether among them there is a unit $\xi_3 = \varepsilon_3$ for which at least one of the $t-2$ symbols

$$\left\{\frac{\varepsilon_3, \mu}{\mathfrak{l}_1}\right\}, \dots, \left\{\frac{\varepsilon_3, \mu}{\mathfrak{l}_{t-2}}\right\}$$

turns out to be different from 1. Proceeding in this way we obtain eventually a number r^* and a set of r^* units $\varepsilon_1, \dots, \varepsilon_{r^*}$ of $k(\zeta)$ such that, by a suitable arrangement of the prime ideals $\mathfrak{l}_1, \dots, \mathfrak{l}_t$ we have the equations

$$\left.\begin{array}{l}
\left\{\frac{\varepsilon_1,\mu}{\mathfrak{l}_t}\right\}=\zeta \\
\left\{\frac{\varepsilon_2,\mu}{\mathfrak{l}_t}\right\}=1, \quad \left\{\frac{\varepsilon_2,\mu}{\mathfrak{l}_{t-1}}\right\}=\zeta \\
\left\{\frac{\varepsilon_3,\mu}{\mathfrak{l}_t}\right\}=1, \quad \left\{\frac{\varepsilon_3,\mu}{\mathfrak{l}_{t-1}}\right\}=1, \quad \left\{\frac{\varepsilon_3,\mu}{\mathfrak{l}_{t-2}}\right\}=\zeta \\
\qquad\qquad\qquad\qquad \cdots\cdots \\
\left\{\frac{\varepsilon_{r^*},\mu}{\mathfrak{l}_t}\right\}=1, \quad \left\{\frac{\varepsilon_{r^*},\mu}{\mathfrak{l}_{t-1}}\right\}=1, \quad \left\{\frac{\varepsilon_{r^*},\mu}{\mathfrak{l}_{t-2}}\right\}=1, \quad \ldots \quad \left\{\frac{\varepsilon_{r^*},\mu}{\mathfrak{l}_{t-r^*+1}}\right\}=\zeta
\end{array}\right\} \tag{32.19}$$

and further, for each unit ξ which satisfies the r^* equations

$$\left\{\frac{\xi,\mu}{\mathfrak{l}_t}\right\}=1, \left\{\frac{\xi,\mu}{\mathfrak{l}_{t-1}}\right\}=1, \ldots, \left\{\frac{\xi,\mu}{\mathfrak{l}_{t-r^*+1}}\right\}=1$$

the remaining $r=t-r^*$ symbols

$$\left\{\frac{\xi,\mu}{\mathfrak{l}_1}\right\}, \ldots, \left\{\frac{\xi,\mu}{\mathfrak{l}_r}\right\}$$

all have the value 1.

Let ν be the number in $k(\zeta)$ which was derived earlier from the ideal $\mathfrak{J}$. Multiply ν by suitable powers of the units $\varepsilon_1, \ldots, \varepsilon_{r^*}$ so that the product $\bar{\nu}$ so obtained satisfies the equations

$$\left\{\frac{\bar{\nu},\mu}{\mathfrak{l}_t}\right\}=1, \left\{\frac{\bar{\nu},\mu}{\mathfrak{l}_{t-1}}\right\}=1, \ldots, \left\{\frac{\bar{\nu},\mu}{\mathfrak{l}_{t-r^*+1}}\right\}=1;$$

then the $r=t-r^*$ units

$$\chi_1(\mathfrak{J})=\left\{\frac{\bar{\nu},\mu}{\mathfrak{l}_1}\right\}, \ldots, \chi_r(\mathfrak{J})=\left\{\frac{\bar{\nu},\mu}{\mathfrak{l}_r}\right\}$$

form the *character set* of the ideal $\mathfrak{J}$. This set is completely and uniquely determined by the ideal $\mathfrak{J}$. In Sect. 151 we shall show that we always have $r^* < t$ and hence $r \geq 1$.

§150. The Character Set of an Ideal Class and the Notion of Genus

From Theorem 151 and the remarks following it on pp. 250-1 we deduce at once the following result.

Theorem 160. *All the ideals belonging to a single ideal class of a regular Kummer field have the same character set.*

In this way we associate a character set with each ideal class. As we did in Sect. 66 for quadratic fields we shall say that all ideal classes with the same character set form a *genus* and in particular we define the *principal genus* to be the totality of all the ideal classes for which the character set consists entirely of the unit 1. Since the character set of the principal class clearly has this property the principal class always belongs to the principal genus. From the first formulæ in (29.9) on p. 240 and (29.12) on p. 242 we deduce easily that if G and G' are any two genera and every class in G is multiplied by every class in G' then the totality of all these products again forms a genus; we call it the *product* of the genera G and G'. The character set of the product is obtained by multiplying the corresponding characters of the two genera G and G'.

From the above definition of genera it is clear that the relative conjugate classes $SC, \ldots, S^{l-1}C$ of an ideal class C belong to the same genus as C itself. From this it follows that the $(1-S)$-th symbolic power C^{1-S} of a class C always belongs to the principal genus. Finally it is clear that all the genera of a Kummer field consist of the same number of ideal classes.

§151. Upper Bound for the Degree of the Class Bundle of All Ambig Classes

The important question now presents itself, as in the theory of quadratic fields, whether a set of r arbitrarily given l-th roots of unity can be the character set for a genus in a Kummer field. We shall find the complete answer in Chapter 34. In this and the following section we shall simply prove some lemmas which will be necessary later.

Lemma 33. *If t and n have the same meaning as in Theorem* 159 *and r is the number of characters which determine the genus of a class of the Kummer field then*

$$t + n - \tfrac{1}{2}(l+1) \leq r - 1.$$

Proof. Let $\varepsilon_1, \ldots, \varepsilon_{r^*}$ be the r^* units of the field $k(\zeta)$ which were introduced in Sect. 149. Then $r = t - r^*$. Next let $\vartheta_1, \ldots, \vartheta_n$ be a basis for the unit bundle in $k(\zeta)$ which consists of all the units in $k(\zeta)$ which are relative norms of numbers in K. We now suppose that there were a relation between the $r^* + n$ units $\varepsilon_1, \ldots, \varepsilon_{r^*}, \vartheta_1, \ldots, \vartheta_n$ of the form

$$\varepsilon_1^{a_1} \cdots \varepsilon_{r^*}^{a_{r^*}} \vartheta_1^{b_1} \cdots \vartheta_n^{b_n} = \varepsilon^l \tag{32.20}$$

where $a_1, \ldots, a_{r^*}, b_1, \ldots, b_n$ are rational integers not all divisible by l and ε is a unit of $k(\zeta)$. Then for $u = 1, 2, \ldots, t$ it would follow that

$$\left\{\frac{\varepsilon_1^{a_1}\cdots\varepsilon_{r^*}^{a_{r^*}}\vartheta_1^{b_1}\cdots\vartheta_n^{b_n},\mu}{\mathfrak{l}_u}\right\}=1.$$

When we recall that the units $\vartheta_1, \ldots, \vartheta_n$ are all relative norms of numbers in K, and hence $\left\{\frac{\vartheta_v,\mu}{\mathfrak{l}_u}\right\}=1$ for $u = 1, 2, \ldots, t$ and $v = 1, 2, \ldots, n$, we see that we would have

$$\left\{\frac{\varepsilon_1^{a_1}\cdots\varepsilon_{r^*}^{a_{r^*}},\mu}{\mathfrak{l}_u}\right\}=1$$

for $u = 1, 2, \ldots, t$. According to the formulæ for the units $\varepsilon_1, \ldots, \varepsilon_{r^*}$ this is possible only if the exponents $a_1, \ldots, a_{r^*}$ are all divisible by l. Thus the relation (32.20) would take the form

$$\vartheta_1^{b_1}\cdots\vartheta_n^{b_n}=(\varepsilon^*)^l$$

where ε^* is again a unit in $k(\zeta)$. But, since $\vartheta_1, \ldots, \vartheta_n$ form a basis for a unit bundle in $k(\zeta)$, such a relation can hold only if all the exponents $b_1, \ldots, b_n$ are divisible by l. From this it follows that no relation of the form (32.20) can in fact hold; so the units $\varepsilon_1, \ldots, \varepsilon_{r^*}, \vartheta_1, \ldots, \vartheta_n$ form the basis of a unit bundle. The degree of this unit bundle is $r^* + n$ and since the degree of a unit bundle cannot exceed $\frac{1}{2}(l-1)$ we have $r^* + n \le \frac{1}{2}(l-1)$; from this we deduce the assertion of Lemma 33.

Since $t+n-\frac{1}{2}(l+1) \ge 0$ it follows in particular that $r^* < t$ and so $r \ge 1$.

§152. Complexes in a Regular Kummer Field

Let h be the number of ideal classes in the regular cyclotomic field $k(\zeta)$; then in the Kummer field $K = k(\sqrt[l]{\mu}, \zeta)$ there are precisely h distinct ideal classes which contain ideals of $k(\zeta)$. To see this we notice that every ideal class of $k(\zeta)$ obviously gives rise to a class of K of the type under consideration; if two distinct classes c_1 and c_2 of $k(\zeta)$ were to contain ideals which are equivalent in K then an ideal $\mathfrak{i}$ of $k(\zeta)$ in the class c_1/c_2 would have to become a principal ideal in K. According to Theorem 153 $\mathfrak{i}$ must also be a principal ideal in $k(\zeta)$, which contradicts the hypothesis that $c_1 \neq c_2$.

Let now C be any ideal class in K and $c_1, \ldots, c_h$ the h classes of K which contain ideals of $k(\zeta)$. Then the collection of classes $c_1C, \ldots, c_hC$ is called a *complex*. The complex consisting of the h classes $c_1, \ldots, c_h$ is called the *principal complex* and is denoted by 1. Clearly all h classes of a complex P belong to the same genus; this genus will be called the *genus of the complex* P.

If one of the classes in a complex P is ambig then all the classes of P are ambig; in this case we say that P is an *ambig complex*.

If P and P' are ambig complexes and every class in P is multiplied by every class in P' then the collection of all the products so formed is again a complex; we call it the *product* of the complexes P and P' and denote it by

PP'. If C is a class in a complex P then the complex to which the relative conjugate class SC belongs will be denoted by SP; the complex Q which, on multiplication by SP, yields the complex P will be called the $(1-S)$*-th symbolic power* of P and denoted by $Q = P^{1-S}$.

If in particular the $(1-S)$-th symbolic power of a complex P is the principal complex 1 then P is an ambig complex. For, if C is a class in P, then, since $P^{1-S} = 1$, we must have $C^{1-S} = c$, where c is one of the h classes $c_1, \ldots, c_h$. Taking relative norms of both sides of this equation we obtain the result that $1 = c^l$. Since we also have $c^h = 1$ we deduce easily that $c = 1$, i.e. $C^{1-S} = 1$. Hence C is an ambig class and P an ambig complex.

§153. An Upper Bound for the Number of Genera in a Regular Kummer Field

Lemma 34. *If t and n have the same meaning as in Theorem* 159 *and g is the number of genera of the regular Kummer field K then we have*

$$g \leq l^{t+n-\frac{1}{2}(l+1)}.$$

Proof. If g is the number of genera in the Kummer field K then, as we see at once from the definition of the genus of a complex, the complexes of K also fall into precisely g genera. If f is the number of complexes in the principal genus then the total number of complexes, which we denote by M, is given by $M = fg$.

We shall now determine the number a of ambig complexes. To this end we recall that, according to Theorem 159, the degree of the class bundle consisting of all ambig classes is $t' = t + n - \frac{1}{2}(l+1)$. Let $A_1, \ldots, A_{t'}$ be a basis for this class bundle. Then the expression

$$A_1^{u_1} \cdots A_{t'}^{u_{t'}},$$

where the exponents $u_1, \ldots, u_{t'}$ run independently through the range $0, 1, \ldots, l-1$, represents ambig classes which lie in different complexes. So there are precisely $l^{t'}$ complexes determined by these classes. Every ambig class A can be represented in the form

$$A = A_1^{a_1} \cdots A_{t'}^{a_{t'}} c$$

where $a_1, \ldots, a_{t'}$ are rational integer exponents and c is an ideal class of $k(\zeta)$. We recall now that the l-th powers of the ambig classes $A_1, \ldots, A_{t'}$ are classes containing ideals of $k(\zeta)$. It follows that A must necessarily belong to one of the $l^{t'}$ complexes determined above. Hence the required number a is given by $a = l^{t'} = l^{t+n-\frac{1}{2}(l+1)}$.

It follows from the definitions in Sect. 150 and Sect. 152 that the $(1-S)$-th symbolic power of every complex is in the principal genus. We now fix our attention on those complexes of the principal genus which are $(1-S)$-th symbolic powers of complexes; suppose there are f' of them, denoted by $P_1, \ldots, P_{f'}$ and let $P_1 = G_1^{1-S}, \ldots, P_{f'} = G_{f'}^{1-S}$ where $G_1, \ldots, G_{f'}$ are complexes of K. If P is any complex of K then P^{1-S} must be one of the f' complexes $P_1, \ldots, P_{f'}$; say $P^{1-S} = P_v$. Then we have $P^{1-S} = G_v^{1-S}$, whence $(PG_v^{-1})^{1-S} = 1$ and so PG_v^{-1} is an ambig complex A, i.e. $P = AG_v$. Thus, as A runs through all ambig complexes and G_v through the f' complexes $G_1, \ldots, G_{f'}$, the expression AG_v represents all complexes. It is also clear that for each complex this representation is possible in one way only. Hence the total number of complexes is $M = af'$. Combining this result with the equation $M = gf$ obtained above we have $af' = gf$; since $f' \le f$ we deduce that $g \le a = l^{t+n-\frac{1}{2}(l+1)}$ as asserted in Lemma 34.

We have the following immediate consequence of Lemmas 33 and 34.

Lemma 35. *If in a regular Kummer field the number of characters which determine the genus of a class is r then the number g of genera of the field does not exceed l^{r-1}.*

33. The l-th Power Reciprocity Law in Regular Cyclotomic Fields

§154. The l-th Power Reciprocity Law and the Supplementary Laws

The theory of Kummer fields which we have developed thus far gives us the resources required for the proof of certain fundamental laws concerning l-th power residues in regular cyclotomic fields which correspond to the quadratic reciprocity law in the domain of rational numbers and include as a special case the Eisenstein reciprocity law (Theorem 140) between an arbitrary number in $k(\zeta)$ and a rational number which we developed in Sect. 115. In order to be able to state these laws for l-th power residues in their simplest form we generalise the symbol $\left\{\frac{\mu}{\mathfrak{w}}\right\}$ defined in Sect. 113 and Sect. 127 as follows.

Let h be the number of ideal classes in $k(\zeta)$; let h^* be a positive rational integer such that $hh^* \equiv 1 \pmod{l}$. If $\mathfrak{p}$ is any prime ideal of $k(\zeta)$ distinct from $\mathfrak{l}$ then $\mathfrak{p}^{hh^*}$ is a principal ideal in $k(\zeta)$; we set $\mathfrak{p}^{hh^*} = (\pi)$ where π is an integer of $k(\zeta)$ and we suppose that π is primary (this is possible as a result of Theorem 157). Such a number π will be called a *primary number* for $\mathfrak{p}$. According to a remark on p. 267 every primary unit of $k(\zeta)$ is the l-th power of a unit in $k(\zeta)$; so π has a completely determined power character with respect to every prime ideal of $k(\zeta)$ distinct from $\mathfrak{p}$. If now $\mathfrak{q}$ is any prime ideal of $k(\zeta)$ distinct from $\mathfrak{p}$ and from $\mathfrak{l}$ then we define the symbol $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}$ by the formula

$$\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} = \left\{\frac{\pi}{\mathfrak{q}}\right\}.$$

The symbol $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}$ is thus an l-th root of unity uniquely determined by the two prime ideals $\mathfrak{p}$ and $\mathfrak{q}$. Using this symbol we can state the following result.

Theorem 161. *Let $\mathfrak{p}$ and $\mathfrak{q}$ be prime ideals of the regular cyclotomic field $k(\zeta)$, distinct from one another and from the prime ideal $\mathfrak{l}$. Then*

$$\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\}$$

(the so-called l-th power reciprocity law). Further, if ξ is any unit in $k(\zeta)$ and π is a primary number for the prime ideal $\mathfrak{p}$, then we have

$$\left\{\frac{\xi}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \xi}{\mathfrak{l}}\right\} \quad \text{and} \quad \left\{\frac{\lambda}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \lambda}{\mathfrak{l}}\right\}$$

(the so-called supplementary laws for the l-th power reciprocity law) (Kummer (10, 12, 18, 19, 20, 21)).

We develop the proof of this fundamental theorem step by step in the following sections of this chapter by applying to particular regular Kummer fields the theorems and lemmas obtained in the previous chapter.

§155. Prime Ideals of First and Second Kind in a Regular Cyclotomic Field

It is useful for the development which follows to distinguish two types of prime ideals in $k(\zeta)$. A prime ideal $\mathfrak{p}$ of $k(\zeta)$ distinct from $\mathfrak{l}$ modulo which not every unit of $k(\zeta)$ is an l-th power residue is called a *prime ideal of the first kind*; on the other hand a prime ideal $\mathfrak{q}$ of $k(\zeta)$ distinct from $\mathfrak{l}$ is called a *prime ideal of the second kind* if all units of $k(\zeta)$ are l-th power residues modulo $\mathfrak{q}$ (*Kummer* (20)). We prove first the following lemmas.

Lemma 36. *If ξ and ε are units of the regular cyclotomic field $k(\zeta)$ and we set $\lambda = 1 - \zeta$, $\mathfrak{l} = (\lambda)$ then we have*

$$\left\{\frac{\xi, \varepsilon}{\mathfrak{l}}\right\} = 1 \quad \textit{and} \quad \left\{\frac{\lambda, \varepsilon}{\mathfrak{l}}\right\} = 1.$$

Proof. If ε is the l-th power of a unit in $k(\zeta)$ then the equations stated in the lemma are obviously satisfied. Otherwise $\sqrt[l]{\varepsilon}$ determines a Kummer field $k(\sqrt[l]{\varepsilon}, \zeta)$ of the type considered at the end of Sect. 147. Hence all units in $k(\zeta)$ and also the number λ are relative norms of numbers in $k(\sqrt[l]{\varepsilon}, \zeta)$; so the equations in the lemma follow from Theorem 151.

If we prefer to use here only the case $\mathfrak{w} = \mathfrak{l}$ of Theorem 151 considered in detail on pp. 249-250, where the number μ in question is congruent to $1 + \lambda$ modulo $\mathfrak{l}^2$, then we prove the last result first in the case where the unit ε is ζ^{l-1}; then it follows that $\left\{\frac{\xi, \zeta}{\mathfrak{l}}\right\} = 1$ and $\left\{\frac{\lambda, \zeta}{\mathfrak{l}}\right\} = 1$. Next, if ε is any unit in $k(\zeta)$, we determine an l-th root of unity ζ^* such that $\zeta^* \varepsilon^{l-1} \equiv 1 + \lambda$ (mod $\mathfrak{l}^2$). If we take $\zeta^* \varepsilon^{l-1}$ instead of ε in the above proof it follows by means

of the second formula in (29.12) on p. 242 that we have $\left\{\frac{\xi,\varepsilon}{\mathfrak{l}}\right\} = 1$ and similarly $\left\{\frac{\lambda,\varepsilon}{\mathfrak{l}}\right\} = 1$.

Lemma 37. *If $\mathfrak{p}$ is a prime ideal of the first kind and π a primary number for $\mathfrak{p}$ then there is at least one unit ε in $k(\zeta)$ for which*

$$\left\{\frac{\varepsilon,\pi}{\mathfrak{l}}\right\} \neq 1.$$

If $\mathfrak{q}$ is a prime ideal of the second kind and κ a primary number for $\mathfrak{q}$ then for every unit ξ of $k(\zeta)$ we have

$$\left\{\frac{\xi,\kappa}{\mathfrak{l}}\right\} = 1.$$

Proof. To prove the first assertion of the lemma let us suppose, to the contrary, that for every unit ξ of $k(\zeta)$ we have

$$\left\{\frac{\xi,\pi}{\mathfrak{l}}\right\} = 1.$$

We write $\pi \equiv a + b\lambda^e \pmod{\mathfrak{l}^{e+1}}$ where a and b are rational integers and e is the greatest exponent not exceeding $l-1$ for which we can have such a congruence. Since π is a primary number we must have $e > 1$ and $\pi \cdot s^{\frac{1}{2}(l-1)}\pi$ must be congruent to a rational integer modulo l, where $s^{\frac{1}{2}(l-1)}$ is the automorphism $(\zeta : \zeta^{-1})$ in the group of the cyclotomic field $k(\zeta)$. Since $s^{\frac{1}{2}(l-1)}\lambda \equiv -\lambda \pmod{\mathfrak{l}^2}$ we have

$$\pi \cdot s^{\frac{1}{2}(l-1)}\pi \equiv (a + b\lambda^e)(a + b(-\lambda)^e) \pmod{\mathfrak{l}^{e+1}}$$

and from this it follows that if $e < l-1$ then the exponent e must be odd.

In the proof of Lemma 29 we found that the $l^* = \frac{1}{2}(l-3)$ units denoted there by $\varepsilon_1, \ldots, \varepsilon_{l^*}$ satisfy the conditions

$$\left.\begin{array}{lcll} l^{(u)}(\varepsilon_t) & \equiv & 0 \pmod{l} & (u \neq 2t) \\ l^{(2t)}(\varepsilon_t) & \not\equiv & 0 \pmod{l} & \end{array}\right\} \left(\begin{array}{lcl} t & = & 1, 2, \ldots, l^*; \\ u & = & 1, 2, \ldots, l-2. \end{array}\right)$$

In the first equation of this proof take ξ to be in turn $\varepsilon_1, \ldots, \varepsilon_{l^*}$. Then, from the definition (29.11) of the symbol $\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}$ on p. 242 and the extensions given there, we have the congruences

$$l^{(l-2)}(\pi^{l-1}) \equiv 0, l^{(l-4)}(\pi^{l-1}) \equiv 0, l^{(l-6)}(\pi^{l-1}) \equiv 0, \ldots, l^{(3)}(\pi^{l-1}) \equiv 0 \pmod{l}$$

and these show us that in the congruence $\pi \equiv a+b\lambda^e \pmod{\mathfrak{l}^{e+1}}$ the exponent e can have none of the values $l-2$, $l-4$, $l-6$, $\ldots$, 3. Taking this together

with the condition on e which we found above we see that we must have $e = l-1$. Since $\lambda^{l-1} \equiv -l \pmod{\mathfrak{l}^l}$ we have $\pi \equiv a - bl \pmod{\mathfrak{l}^l}$ and hence the norm of π satisfies the congruence

$$n(\pi) \equiv (a-bl)^{l-1} \equiv \pi^{l-1} \pmod{\mathfrak{l}^l}.$$

On the other hand we conclude from the definition of the symbol on p. 242, having regard to Lemma 24, that

$$\left\{\frac{\zeta, \pi}{\mathfrak{l}}\right\} = \zeta^{(1-n(\pi))/l},$$

and, since the symbol on the left hand side has the value 1, it follows that $n(\pi) \equiv 1 \pmod{l^2}$, i.e. $\pi^{l-1} \equiv 1 \pmod{\mathfrak{l}^l}$ or $\pi^l \equiv \pi \pmod{\mathfrak{l}^l}$. According to Theorem 148 this last congruence implies that the Kummer field $k(\sqrt[l]{\pi}, \zeta)$ determined by $\sqrt[l]{\pi}$ has relative discriminant prime to $\mathfrak{l}$; hence $\mathfrak{p}$ is the only prime ideal dividing the relative discriminant of $k(\sqrt[l]{\pi}, \zeta)$. If we set $\mathfrak{p} = \mathfrak{P}^l$ we see that $\mathfrak{P}$ is the only ambig prime ideal of this field. Since $\sqrt[l]{\pi} = \mathfrak{P}^{hh^*} = \mathfrak{P}\mathfrak{p}^{(hh^*-1)/l}$ it follows that $\mathfrak{P}$ is equivalent to an ideal of $k(\zeta)$. Thus the class bundle of the field $k(\sqrt[l]{\pi}, \zeta)$ consisting of all ambig prime ideals has degree 0. Since for this field the number t of ambig ideals is 1, it follows from Theorem 158 (where m has the meaning described in that theorem) that we have $1 + m - \frac{1}{2}(l+1) = 0$, i.e. $m = \frac{1}{2}(l-1)$. It follows that every unit ξ of $k(\zeta)$ is the relative norm of a unit in $k(\sqrt[l]{\pi}, \zeta)$; hence, by Theorem 151, we have $\left\{\frac{\xi, \pi}{\mathfrak{p}}\right\} = 1$ and therefore, since $\left\{\frac{\xi, \pi}{\mathfrak{p}}\right\} = \left\{\frac{\xi^{hh^*}}{\mathfrak{p}}\right\} = \left\{\frac{\xi}{\mathfrak{p}}\right\}$, we have $\left\{\frac{\xi}{\mathfrak{p}}\right\} = 1$ for every unit ξ of $k(\zeta)$, contrary to our assumption that $\mathfrak{p}$ is a prime ideal of the first kind.

To prove the second assertion of Lemma 37 we consider, as in the proof of Lemma 36, the Kummer field $k(\sqrt[l]{\xi}, \zeta)$ where ξ is a unit in $k(\zeta)$ which is not the l-th power of a unit in $k(\zeta)$. As we proved at the end of Sect. 147, every unit of $k(\zeta)$ is the relative norm of a unit in $k(\sqrt[l]{\xi}, \zeta)$ and hence, in the case of this field, the two unit bundles described in Theorem 158 and Theorem 159 have the same degree

$$m = n = \tfrac{1}{2}(l-1).$$

Since for this field we also have $t = 1$ it follows from Lemma 34 that $g \leq 1$. So $g = 1$, i.e. all ideal classes of the field $k(\sqrt[l]{\xi}, \zeta)$ belong to the principal genus. Since $\mathfrak{q}$ is a prime ideal of the second kind we have $\left\{\frac{\xi}{\mathfrak{q}}\right\} = 1$ and hence, by Theorem 149, $\mathfrak{q}$ splits into l distinct prime factors in $k(\sqrt[l]{\xi}, \zeta)$. Let $\mathfrak{Q}$ be one of these prime factors of $\mathfrak{q}$. The character set of a nonzero number α of the field $k(\zeta)$ in $k(\sqrt[l]{\xi}, \zeta)$ consists of a single character $\left\{\frac{\alpha, \xi}{\mathfrak{l}}\right\}$; according to Lemma 36 this always has the value 1 if α is chosen to be a unit of $k(\zeta)$. The character of the prime ideal $\mathfrak{Q}$ in $k(\sqrt[l]{\xi}, \zeta)$ thus has the value $\left\{\frac{\kappa, \xi}{\mathfrak{l}}\right\}$ and by

the results proved earlier this has the value 1. This completes the proof of Lemma 37.

Here again, if we wish to suppose that Theorem 151 for $\mathfrak{w} = \mathfrak{l}$ has been proved only in the case of a field $k(\sqrt[l]{\mu}, \zeta)$ for which $\mu \equiv 1 + \lambda \pmod{\mathfrak{l}^2}$ then the classification of the genera and in particular Lemma 34 hold only for this case. So to prove the second assertion of Lemma 37 we must choose first $\xi = \zeta^{l-1}$ and then $\xi = \zeta^* \varepsilon^{l-1}$ where ε is any unit in $k(\zeta)$ and ζ^* is an l-th root of unity such that $\zeta^* \varepsilon^{l-1} \equiv 1 + \lambda \pmod{\mathfrak{l}^2}$. By combining the two results obtained from these choices we obtain the second assertion of the lemma in its full generality.

§156. Lemmas on Prime Ideals of the First Kind in Regular Cyclotomic Fields

We prove the following sequence of lemmas on prime ideals of the first kind in the field $k(\zeta)$.

Lemma 38. *Let $\mathfrak{p}$ be a prime ideal of the first kind in a regular cyclotomic field $k(\zeta)$; let π be a primary number for $\mathfrak{p}$. If there exists a unit ε of $k(\zeta)$ such that*

$$\left\{\frac{\pi, \varepsilon}{\mathfrak{l}}\right\} \neq 1 \quad \textit{and} \quad \left\{\frac{\varepsilon}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \varepsilon}{\mathfrak{l}}\right\}$$

then for every unit ξ of $k(\zeta)$ we have

$$\left\{\frac{\xi}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \xi}{\mathfrak{l}}\right\}.$$

Proof. Since $\mathfrak{p}$ is a prime ideal of the first kind it follows from the proof of Lemma 37 that the Kummer field $k(\sqrt[l]{\pi}, \zeta)$ determined by $\sqrt[l]{\pi}$ has two ambig prime ideals $\mathfrak{L}$ and $\mathfrak{P}$, namely those whose l-th powers are $\mathfrak{l}$ and $\mathfrak{p}$ respectively. Since the ambig ideal $\mathfrak{P}$ is obviously a principal ideal in $k(\sqrt[l]{\pi}, \zeta)$ it follows that for this field the class bundle of all the ambig ideals has degree 0 or 1 according as $\mathfrak{L}$ is a principal ideal or not. Thus, according to Theorem 158, the number $2 + m - \frac{1}{2}(l+1)$ has the value 0 or 1, where m is the degree of the unit bundle consisting of relative norms of units in $k(\sqrt[l]{\pi}, \zeta)$. So $m = \frac{1}{2}(l-3)$ or $m = \frac{1}{2}(l-1)$. Since, by hypothesis, we have $\left\{\frac{\pi, \varepsilon}{\mathfrak{l}}\right\} \neq 1$ it follows from Theorem 151 that ε is not the relative norm of a unit in $k(\sqrt[l]{\pi}, \zeta)$; so we must have $m = \frac{1}{2}(l-3)$. Thus every unit ξ of $k(\zeta)$ can be represented in the form $\xi = \varepsilon^a \vartheta$ where a is a rational integer exponent and ϑ is a unit which is the relative norm of a unit in $k(\sqrt[l]{\pi}, \zeta)$. From this we see, according to Theorem 151, that

$$\left\{\frac{\vartheta,\pi}{\mathfrak{l}}\right\}=1,\quad \left\{\frac{\vartheta,\pi}{\mathfrak{p}}\right\}=\left\{\frac{\vartheta}{\mathfrak{p}}\right\}=1$$

and hence also $\left\{\frac{\pi,\vartheta}{\mathfrak{l}}\right\}=\left\{\frac{\vartheta}{\mathfrak{p}}\right\}$. From this it follows, using the second formula in (29.12) on p.246, that we also have $\left\{\frac{\pi,\xi}{\mathfrak{l}}\right\}=\left\{\frac{\xi}{\mathfrak{p}}\right\}$. This completes the proof of Lemma 38.

If we apply Theorem 151 for $\mathfrak{w}=\mathfrak{l}$ only in the case of a field $k(\sqrt[l]{\mu},\zeta)$ for which $\mu\equiv 1+\lambda \pmod{\mathfrak{l}^2}$ then we determine an l-th root of unity ζ^* such that $\zeta^*\pi^{l-1}\equiv 1+\lambda \pmod{\mathfrak{l}^2}$ and then, replacing the field $k(\sqrt[l]{\pi},\zeta)$ by the field $k(\sqrt[l]{\zeta^*\pi^{l-1}},\zeta)$, proceed exactly as in the proof described above. Finally, if we make use of Lemma 36, we complete the proof of Lemma 38.

Lemma 39. *Let $\mathfrak{p}$, $\mathfrak{p}^*$ be prime ideals of $k(\zeta)$ of the first kind; let π, π^* be primary numbers for $\mathfrak{p}$, $\mathfrak{p}^*$ respectively. If for every unit ξ of $k(\zeta)$ we have*

$$\left\{\frac{\xi}{\mathfrak{p}}\right\}=\left\{\frac{\pi,\xi}{\mathfrak{l}}\right\}\quad \textit{and}\quad \left\{\frac{\xi}{\mathfrak{p}^*}\right\}=\left\{\frac{\pi^*,\xi}{\mathfrak{l}}\right\}$$

then

$$\left\{\frac{\mathfrak{p}}{\mathfrak{p}^*}\right\}=\left\{\frac{\mathfrak{p}^*}{\mathfrak{p}}\right\}.$$

Proof. Since $\mathfrak{p}^*$ is a prime ideal of the first kind we can find a unit ε in $k(\zeta)$ such that $\left\{\frac{\varepsilon\pi}{\mathfrak{p}^*}\right\}=1$. We now consider the Kummer field $k(\sqrt[l]{\varepsilon\pi},\zeta)$. Since the relative discriminant of this field has only the two prime factors $\mathfrak{l}$ and $\mathfrak{p}$ the character set of a nonzero number α of $k(\zeta)$ for this field consists of the two characters $\left\{\frac{\alpha,\varepsilon\pi}{\mathfrak{l}}\right\}$ and $\left\{\frac{\alpha,\varepsilon\pi}{\mathfrak{p}}\right\}=\left\{\frac{\alpha}{\mathfrak{p}}\right\}$. Since $\left\{\frac{\varepsilon\pi}{\mathfrak{p}^*}\right\}=1$ the prime ideal $\mathfrak{p}^*$ factorises in $k(\sqrt[l]{\varepsilon\pi},\zeta)$; let $\mathfrak{P}^*$ be a factor of $\mathfrak{p}^*$ in this field. To form the character set of $\mathfrak{P}^*$ we bear in mind that $\mathfrak{p}$ is a prime ideal of the first kind; so we can find a unit ε^* in $k(\zeta)$ for which $\left\{\frac{\varepsilon^*\pi^*}{\mathfrak{p}}\right\}=1$ and the character set of $\mathfrak{P}^*$ consists of the single character $\left\{\frac{\varepsilon^*\pi^*,\varepsilon\pi}{\mathfrak{l}}\right\}$. We thus deduce from Lemma 35 that for the field $k(\sqrt[l]{\varepsilon\pi},\zeta)$ we have $g\leq 1$, i.e. in this field every ideal class belongs to the principal genus and so the character last mentioned has the value 1. We now have $\left\{\frac{\varepsilon\pi}{\mathfrak{p}^*}\right\}=1$ and so, according to the formula on p. 199, we have

$$\left\{\frac{\mathfrak{p}}{\mathfrak{p}^*}\right\}=\left\{\frac{\varepsilon}{\mathfrak{p}^*}\right\}^{-1}. \tag{33.1}$$

Further, $\left\{\frac{\varepsilon^*\pi^*}{\mathfrak{p}}\right\}=1$, i.e.

$$\left\{\frac{\mathfrak{p}^*}{\mathfrak{p}}\right\} = \left\{\frac{\varepsilon^*}{\mathfrak{p}}\right\}^{-1} \tag{33.2}$$

and finally $\left\{\frac{\varepsilon^*\pi^*, \varepsilon\pi}{\mathfrak{l}}\right\} = 1$ or, by using (29.12) on p. 242,

$$\left\{\frac{\varepsilon^*, \varepsilon}{\mathfrak{l}}\right\}\left\{\frac{\varepsilon^*, \pi}{\mathfrak{l}}\right\}\left\{\frac{\pi^*, \varepsilon}{\mathfrak{l}}\right\}\left\{\frac{\pi^*, \pi}{\mathfrak{l}}\right\} = 1.$$

Since by Lemma 36 we have $\left\{\frac{\varepsilon^*, \varepsilon}{\mathfrak{l}}\right\} = 1$ and by Lemma 30 $\left\{\frac{\pi^*, \pi}{\mathfrak{l}}\right\} = 1$, the last formula yields

$$\left\{\frac{\pi, \varepsilon^*}{\mathfrak{l}}\right\} = \left\{\frac{\pi^*, \varepsilon}{\mathfrak{l}}\right\}. \tag{33.3}$$

According to our hypothesis we have

$$\left\{\frac{\pi, \varepsilon^*}{\mathfrak{l}}\right\} = \left\{\frac{\varepsilon^*}{\mathfrak{p}}\right\} \quad \text{and} \quad \left\{\frac{\pi^*, \varepsilon}{\mathfrak{l}}\right\} = \left\{\frac{\varepsilon}{\mathfrak{p}^*}\right\}:$$

then it follows from (33.3) that $\left\{\frac{\varepsilon^*}{\mathfrak{p}}\right\} = \left\{\frac{\varepsilon}{\mathfrak{p}^*}\right\}$ and this equation, taken together with formulæ (33.1) and (33.2) yields the result stated in Lemma 39.

Once again, if we wish to apply Theorem 151 for $\mathfrak{w} = \mathfrak{l}$ only in the case of a field $k(\sqrt[l]{\mu}, \zeta)$ for which $\mu \equiv 1 + \lambda \pmod{\mathfrak{l}^2}$, we should choose the unit ε in the above proof so that we have not only $\left\{\frac{\varepsilon\pi}{\mathfrak{p}^*}\right\} = 1$ but also, for a suitable exponent a prime to l, the congruence $(\varepsilon\pi)^a \equiv 1 + \lambda \pmod{\mathfrak{l}^2}$. It is easily seen that it is always possible to find a unit ε with these properties if $\left\{\frac{\zeta}{\mathfrak{p}^*}\right\} = 1$. If, however, $\left\{\frac{\zeta}{\mathfrak{p}^*}\right\} \neq 1$ and also $\left\{\frac{\pi}{\mathfrak{p}^*}\right\} \neq 1$ then the required condition can be fulfilled by taking for ε a suitable power of ζ. Thus it remains in question whether the condition can be satisfied if we have both $\left\{\frac{\zeta}{\mathfrak{p}^*}\right\} \neq 1$ and $\left\{\frac{\pi}{\mathfrak{p}^*}\right\} = 1$. In this case we interchange the roles played in the above proof by π, $\mathfrak{p}$ on one hand and π^*, $\mathfrak{p}^*$ on the other; then the only case left undecided is that in which we have simultaneously $\left\{\frac{\zeta}{\mathfrak{p}^*}\right\} \neq 1$, $\left\{\frac{\zeta}{\mathfrak{p}}\right\} \neq 1$, $\left\{\frac{\pi}{\mathfrak{p}^*}\right\} = 1$ and $\left\{\frac{\pi^*}{\mathfrak{p}}\right\} = 1$. But in this case we see at once from the latter two relations that the assertion of Lemma 39 holds.

Lemma 40. *Let $\mathfrak{p}$ be a prime ideal of the first kind in $k(\zeta)$ and π a primary number for $\mathfrak{p}$ such that for every unit ξ of $k(\zeta)$ we have*

$$\left\{\frac{\xi}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \xi}{\mathfrak{l}}\right\}.$$

Let $\mathfrak{p}^*$ *be a prime ideal of the first kind distinct from* $\mathfrak{p}$ *such that*

$$\left\{\frac{\mathfrak{p}}{\mathfrak{p}^*}\right\} = \left\{\frac{\mathfrak{p}^*}{\mathfrak{p}}\right\} \neq 1.$$

Then there exists a unit ε *in* $k(\zeta)$ *such that*

$$\left\{\frac{\varepsilon}{\mathfrak{p}^*}\right\} = \left\{\frac{\pi^*, \varepsilon}{\mathfrak{l}}\right\} \neq 1$$

where π^* *is a primary number for* $\mathfrak{p}^*$.

Proof. We proceed at first precisely as in the proof of the preceding lemma and so, by introducing certain units ε and ε^*, obtain the three formulæ (33.1), (33.2) and (33.3). Now, according to the hypothesis of Lemma 40, we have $\left\{\frac{\varepsilon^*}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \varepsilon^*}{\mathfrak{l}}\right\}$; from this and the fact that $\left\{\frac{\mathfrak{p}}{\mathfrak{p}^*}\right\} = \left\{\frac{\mathfrak{p}^*}{\mathfrak{p}}\right\} \neq 1$ we deduce the result of Lemma 40 from the formulæ just mentioned.

If Theorem 151 has been established only in the case where $\mu \equiv 1 + \lambda \pmod{\mathfrak{l}^2}$ we have only to choose the unit ε in the preceding proof in such a way that we have not only $\left\{\frac{\varepsilon\pi}{\mathfrak{p}^*}\right\} = 1$ but also $(\varepsilon\pi)^a \equiv 1 + \lambda \pmod{\mathfrak{l}^2}$ for an exponent a prime to l; such a choice of ε is always possible.

§157. A Particular Case of the Reciprocity Law for Two Ideals

Theorem 162. *If* $\mathfrak{p}$ *and* $\mathfrak{q}$ *are any two prime ideals of a regular cyclotomic field such that* $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} = 1$ *then we also have* $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\} = 1$.

Proof. Let π and κ be primary numbers for $\mathfrak{p}$ and $\mathfrak{q}$ respectively. We consider the Kummer field $k(\sqrt[l]{\mu}, \zeta)$ and distinguish two cases, according as $\mathfrak{p}$ is a prime ideal of the first kind or of the second kind.

In the first case the relative discriminant of $k(\sqrt[l]{\pi}, \zeta)$ is divisible by the two prime ideals $\mathfrak{p}$ and $\mathfrak{l}$ and, according to Lemma 37, there is a unit ε of $k(\zeta)$ for which the character $\left\{\frac{\varepsilon, \pi}{\mathfrak{l}}\right\} \neq 1$. Thus the character set of an ideal in $k(\sqrt[l]{\pi}, \zeta)$ consists of only a single character, i.e. $r = 1$ and hence, by Lemma 35, we also have $g = 1$. Since $\left\{\frac{\pi}{\mathfrak{q}}\right\} = 1$ we see that $\mathfrak{q}$ splits in $k(\sqrt[l]{\pi}, \zeta)$; let $\mathfrak{Q}$ be a prime factor of $\mathfrak{q}$ in this field. Since π and κ are primary numbers it follows from Lemma 30 (p. 267) that $\left\{\frac{\kappa, \pi}{\mathfrak{l}}\right\} = 1$ and since $\mathfrak{Q}$ belongs to the principal genus we have $\left\{\frac{\kappa, \pi}{\mathfrak{l}}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\} = 1$, as asserted in Theorem 162.

If $\mathfrak{p}$ is a prime ideal of the second kind then, according to Lemma 37, we have $\left\{\frac{\xi, \pi}{\mathfrak{l}}\right\} = 1$ for every unit ξ in $k(\zeta)$ and hence, as we showed in the proof of Lemma 37, the relative discriminant of $k(\sqrt[l]{\pi}, \zeta)$ is divisible only by the prime ideal $\mathfrak{p}$. Thus we again have $r = 1$ and $g = 1$. Since $\left\{\frac{\pi}{\mathfrak{q}}\right\} = 1$ it follows that $\mathfrak{q}$ splits in $k(\sqrt[l]{\pi}, \zeta)$. Let $\mathfrak{Q}$ be a prime factor of $\mathfrak{q}$ in this field. Since $\mathfrak{Q}$ belongs to the principal genus and $\left\{\frac{\xi, \pi}{\mathfrak{l}}\right\} = 1$ we have $\left\{\frac{\kappa, \pi}{\mathfrak{p}}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\} = 1$ and so the proof of Theorem 162 is complete.

Once again, if Theorem 151, and so also Lemma 35, are applied for $\mathfrak{w} = \mathfrak{l}$ only in the case of a field $k(\sqrt[l]{\mu}, \zeta)$ for which $\mu \equiv 1 + \lambda \pmod{\mathfrak{l}^2}$ then for the proof of the first of the two cases distinguished above the following supplementary discussion is necessary.

If $\mathfrak{p}$ is any prime ideal and π is a primary number for $\mathfrak{p}$ then from the definition of the symbol $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ and Lemma 24 (p. 242) we have the equation

$$\left\{\frac{\pi, \zeta}{\mathfrak{l}}\right\} = \zeta^{(n(\mathfrak{p})-1)/l} = \left\{\frac{\zeta}{\mathfrak{p}}\right\}. \tag{33.4}$$

If now the prime ideal $\mathfrak{q}$ has the property that $\left\{\frac{\zeta}{\mathfrak{q}}\right\} = 1$ then we determine an l-th root of unity ζ^* such that $\zeta^*\pi^{l-1} \equiv 1 + \lambda \pmod{\mathfrak{l}^2}$ and instead of the Kummer field $k(\sqrt[l]{\pi}, \zeta)$ focus on the field $k(\sqrt[l]{\zeta^*\pi^{l-1}}, \zeta)$. Then we apply the same line of argument as above. We have

$$\left\{\frac{\kappa, \zeta^*\pi^{l-1}}{\mathfrak{l}}\right\} = \left\{\frac{\kappa, \zeta^*}{\mathfrak{l}}\right\}\left\{\frac{\kappa, \pi}{\mathfrak{l}}\right\}^{l-1};$$

as above, $\left\{\frac{\kappa, \pi}{\mathfrak{l}}\right\} = 1$ and we deduce from (33.4) that $\left\{\frac{\kappa, \zeta}{\mathfrak{l}}\right\} = \left\{\frac{\zeta}{\mathfrak{q}}\right\}$; so it follows that $\left\{\frac{\kappa, \zeta^*\pi^{l-1}}{\mathfrak{l}}\right\} = 1$ and hence we conclude that $\left\{\frac{\kappa, \zeta^*\pi^{l-1}}{\mathfrak{p}}\right\} = 1$, i.e. $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\} = 1$.

Suppose on the other hand that $\left\{\frac{\zeta}{\mathfrak{q}}\right\} \neq 1$. Since $\mathfrak{p}$ is a prime ideal of the first kind there exists a unit ε_1 for which $\left\{\frac{\varepsilon_1}{\mathfrak{p}}\right\} \neq 1$; further, by Lemma 37 (p. 291), there is a unit ε_2 for which $\left\{\frac{\varepsilon_2, \pi}{\mathfrak{l}}\right\} \neq 1$. In addition, we can choose both these units ε_1 and ε_2 congruent to $1+\lambda$ modulo $\mathfrak{l}^2$. We now show how to construct a unit ε for which both $\left\{\frac{\varepsilon}{\mathfrak{p}}\right\} \neq 1$ and $\left\{\frac{\varepsilon, \pi}{\mathfrak{l}}\right\} \neq 1$ and which satisfies the congruence $\varepsilon \equiv 1+\lambda \pmod{\mathfrak{l}^2}$: if neither ε_1 nor ε_2 satisfies these conditions then we must have $\left\{\frac{\varepsilon_1, \pi}{\mathfrak{l}}\right\} = 1$ and $\left\{\frac{\varepsilon_2}{\mathfrak{p}}\right\} = 1$; then $\varepsilon = (\varepsilon_1\varepsilon_2)^{\frac{1}{2}(l+1)}$ is a

unit with the desired properties. We now determine a power $\eta = \varepsilon^a$ of the unit ε such that $\left\{\frac{\eta\kappa}{\mathfrak{p}}\right\} = 1$. If $\left\{\frac{\kappa}{\mathfrak{p}}\right\} \neq 1$ then the exponent a must certainly be prime to l and hence we would have $\left\{\frac{\eta, \pi}{\mathfrak{l}}\right\} \neq 1$. Moreover it is clear, since κ is a primary number, that some power of $\eta\kappa$ with an exponent prime to l is congruent to $1 + \lambda$ modulo $\mathfrak{l}^2$. From (33.4) and Lemma 36 (p. 290) it follows that $\left\{\frac{\zeta, \eta\kappa}{\mathfrak{l}}\right\} \neq 1$. Accordingly the Kummer field $k(\sqrt[l]{\eta\kappa}, \zeta)$ has only one genus. Since $\left\{\frac{\eta\kappa}{\mathfrak{p}}\right\} = 1$ the prime ideal $\mathfrak{p}$ splits in this field. If $\mathfrak{P}$ is a prime ideal factor of $\mathfrak{p}$ in this field, the character of $\mathfrak{P}$ is given by the symbol

$$\left\{\frac{\zeta^*\pi, \eta\kappa}{\mathfrak{q}}\right\} = \left\{\frac{\zeta^*\pi}{\mathfrak{q}}\right\},$$

where ζ^* is an l-th root of unity such that $\left\{\frac{\zeta^*\pi, \eta\kappa}{\mathfrak{l}}\right\} = 1$. According to the last equation it follows, since $\left\{\frac{\zeta, \eta}{\mathfrak{l}}\right\} = 1$, that $\left\{\frac{\zeta^*, \kappa}{\mathfrak{l}}\right\}\left\{\frac{\pi, \eta}{\mathfrak{l}}\right\} = 1$; since $\left\{\frac{\pi, \eta}{\mathfrak{l}}\right\} \neq 1$ we must have $\left\{\frac{\zeta^*, \kappa}{\mathfrak{l}}\right\} \neq 1$ also and so, referring to (33.4), we see that $\left\{\frac{\zeta^*}{\mathfrak{q}}\right\} \neq 1$; hence $\zeta^* \neq 1$. Since, however, that single character of the prime ideal $\mathfrak{P}$ must be equal to 1 it follows from the fact that $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} = 1$ that we must also have $\left\{\frac{\zeta^*}{\mathfrak{q}}\right\} = 1$ and this contradicts the conclusion we have just reached.

§158. The Existence of Certain Auxiliary Prime Ideals for Which the Reciprocity Law Holds

From Theorems 152, 140 and 162 it is easy to show the existence of certain prime ideals which we shall make use of in Sect. 159 and Sect. 160. We have the following results.

Lemma 41. *If $\mathfrak{p}$ is any prime ideal of the regular cyclotomic field $k(\zeta)$ then there exists a prime ideal $\mathfrak{r}$ in $k(\zeta)$ such that*

$$\left\{\frac{\zeta}{\mathfrak{r}}\right\} \neq 1 \quad \textit{and} \quad \left\{\frac{\mathfrak{p}}{\mathfrak{r}}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{p}}\right\} \neq 1.$$

Proof. Let h be the class number of $k(\zeta)$ and as in Sect. 149 and Sect. 154 let h^* be a positive rational integer such that $hh^* \equiv 1 \pmod{l}$. Let p be the rational prime number divisible by $\mathfrak{p}$ and $\pi = \mathfrak{p}^{hh^*}$ a primary number for $\mathfrak{p}$. Let $\mathfrak{p}', \mathfrak{p}'', \ldots$ be the prime ideals distinct from $\mathfrak{p}$ and from each other which

are conjugate to $\mathfrak{p}$; let $\pi' = (\mathfrak{p}')^{hh^*}$, $\pi'' = (\mathfrak{p}'')^{hh^*}$, ... be the corresponding conjugates of π in $k(\zeta)$ – these are primary numbers for $\mathfrak{p}'$, $\mathfrak{p}''$, ... respectively. Then we have $p = \mathfrak{p}\mathfrak{p}'\mathfrak{p}'' \cdots$; since, in addition, $p^{hh^*}/\pi\pi'\pi'' \cdots$ must be a unit in $k(\zeta)$ and also primary, it follows from Theorem 156 (p. 265) that this quotient must be the l-th power of a unit ε in $k(\zeta)$, i.e. we have

$$p^{hh^*} = \varepsilon^l \pi\pi'\pi'' \cdots .$$

We now apply Theorem 152 (p. 254), taking

$$\begin{array}{llllll} \alpha_1 = \zeta, & \alpha_2 = \pi, & \alpha_3 = \pi', & \alpha_4 = \pi'', & \alpha_5 = \pi''', & \dots \\ \gamma_1 = \zeta, & \gamma_2 = \zeta, & \gamma_3 = 1, & \gamma_4 = 1, & \gamma_5 = 1, & \dots \end{array}$$

Since ζ is not the l-th power of a unit in $k(\zeta)$ and π, π', π'', ... are powers of prime ideals with exponents prime to l, the conditions of Theorem 152 are satisfied. Hence there is a prime ideal $\mathfrak{r}$ of $k(\zeta)$ such that

$$\left\{\frac{\zeta}{\mathfrak{r}}\right\}^m = \zeta, \quad \left\{\frac{\pi}{\mathfrak{r}}\right\}^m = \zeta, \quad \left\{\frac{\pi'}{\mathfrak{r}}\right\}^m = 1, \quad \left\{\frac{\pi''}{\mathfrak{r}}\right\}^m = 1, \dots$$

for some exponent m prime to l and hence

$$\left\{\frac{\zeta}{\mathfrak{r}}\right\} = \zeta^*, \quad \left\{\frac{\pi}{\mathfrak{r}}\right\} = \zeta^*, \quad \left\{\frac{\pi'}{\mathfrak{r}}\right\} = 1, \quad \left\{\frac{\pi''}{\mathfrak{r}}\right\} = 1, \dots \tag{33.5}$$

where ζ^* is an l-th root of unity other than 1. From (33.5) we obtain the result that $\left\{\frac{p^{hh^*}}{\mathfrak{r}}\right\} = \left\{\frac{\varepsilon^{-l}p^{hh^*}}{\mathfrak{r}}\right\} = \left\{\frac{\pi\pi'\pi''\cdots}{\mathfrak{r}}\right\} = \zeta^*$ and hence, according to Theorem 140 (p. 202), we also have $\left\{\frac{\rho}{p^{hh^*}}\right\} = \zeta^*$ where ρ is a primary number for $\mathfrak{r}$.

From (33.5), using Theorem 162 (p. 296), we must have $\left\{\frac{\rho}{\pi'}\right\} = 1$, $\left\{\frac{\rho}{\pi''}\right\} = 1, \dots$. Since

$$\left\{\frac{\rho}{p^{h^*}}\right\} = \left\{\frac{\rho}{\pi}\right\}\left\{\frac{\rho}{\pi'}\right\}\left\{\frac{\rho}{\pi''}\right\}\cdots$$

it follows that $\left\{\frac{\rho}{\pi}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{p}}\right\} = \zeta^*$. Thus the prime ideal $\mathfrak{r}$ satisfies the requirements of Lemma 41.

Lemma 42. *Let $\mathfrak{p}$ be a prime ideal of the regular cyclotomic field $k(\zeta)$; let π be a primary number for $\mathfrak{p}$. If ε is any unit of $k(\zeta)$ which is not the l-th power of a unit of $k(\zeta)$ then there exists a prime ideal $\mathfrak{r}$ of $k(\zeta)$ such that*

$$\left\{\frac{\varepsilon\pi}{\mathfrak{r}}\right\} = 1 \quad \textit{and} \quad \left\{\frac{\mathfrak{p}}{\mathfrak{r}}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{p}}\right\} \neq 1.$$

Proof. Let π, π', π'', ... have the same meaning as in the proof of Lemma 41. Then, taking

$$\begin{array}{llllll} \alpha_1 = \varepsilon\pi, & \alpha_2 = \pi, & \alpha_3 = \pi', & \alpha_4 = \pi'', & \alpha_5 = \pi''', & \ldots \\ \gamma_1 = 1, & \gamma_2 = \zeta, & \gamma_3 = 1, & \gamma_4 = 1, & \gamma_5 = 1, & \ldots, \end{array}$$

we see that the conditions of Theorem 152 are again satisfied and an argument similar to that in Lemma 41 leads to a prime ideal $\mathfrak{r}$ with the desired property.

§159. Proof of the First Supplementary Law of the Reciprocity Law

In order to prove the first supplementary law for a prime ideal $\mathfrak{p}$ of the first kind we apply Lemma 41 which shows that there is a prime ideal $\mathfrak{r}$ for which

$$\left\{\frac{\zeta}{\mathfrak{r}}\right\} \neq 1 \quad \text{and} \quad \left\{\frac{\mathfrak{r}}{\mathfrak{p}}\right\} = \left\{\frac{\mathfrak{p}}{\mathfrak{r}}\right\} \neq 1$$

and which, in addition, is a prime ideal of the first kind. By (33.4) the prime ideal $\mathfrak{r}$ satisfies the equation

$$\left\{\frac{\zeta}{\mathfrak{r}}\right\} = \zeta^{(n(\mathfrak{r})-1)/l} = \left\{\frac{\rho, \zeta}{\mathfrak{l}}\right\}$$

where ρ is a primary number for $\mathfrak{r}$. Since $\left\{\frac{\zeta}{\mathfrak{r}}\right\} \neq 1$ it follows from Lemma 38 (p. 293) that every other unit ξ of $k(\zeta)$ satisfies the equation

$$\left\{\frac{\xi}{\mathfrak{r}}\right\} = \left\{\frac{\rho, \xi}{\mathfrak{l}}\right\}.$$

Hence all the conditions of Lemma 40 (p. 295) are satisfied if we replace the prime ideals $\mathfrak{p}$, $\mathfrak{p}^*$ in the statement of Lemma 40 by $\mathfrak{r}$ and $\mathfrak{p}$ respectively. Thus, by Lemma 40, there exists a unit ε in $k(\zeta)$ such that $\left\{\frac{\varepsilon}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \varepsilon}{\mathfrak{l}}\right\} \neq 1$ where π is a primary number for $\mathfrak{p}$. It now follows from Lemma 38 (p. 293) that for every other unit ξ in $k(\zeta)$ we have the equation $\left\{\frac{\xi}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \xi}{\mathfrak{l}}\right\}$, as asserted by the first supplementary law.

Next let $\mathfrak{q}$ be a prime ideal of the second kind in $k(\zeta)$. By the definition of such a prime ideal we have $\left\{\frac{\xi}{\mathfrak{q}}\right\} = 1$ for every unit ξ in $k(\zeta)$; and if κ is a primary number for $\mathfrak{q}$ we have $\left\{\frac{\kappa, \xi}{\mathfrak{l}}\right\} = 1$ by Lemma 37 (p. 291). Thus we have again the assertion of the first supplementary law, namely $\left\{\frac{\xi}{\mathfrak{q}}\right\} = \left\{\frac{\kappa, \xi}{\mathfrak{l}}\right\}$.

§160. Proof of the Reciprocity Law for Any Two Prime Ideals

Now that the first supplementary law has been proved in Sect. 159 the reciprocity law for the case of two prime ideals of the first kind follows at once from Lemma 39 (p. 294).

Next let $\mathfrak{p}$ be a prime ideal of the first kind and $\mathfrak{q}$ a prime ideal of the second kind; let π and κ be primary numbers of $\mathfrak{p}$ and $\mathfrak{q}$ respectively. In the case where $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\} = 1$ it follows from Theorem 162 (p. 296) that $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} = 1$ and so we have the reciprocity law for $\mathfrak{p}$ and $\mathfrak{q}$. Suppose now that $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\} = \left\{\frac{\kappa}{\mathfrak{p}}\right\} \neq 1$. Since $\mathfrak{p}$ is of the first kind there is a unit ε such that $\left\{\frac{\varepsilon\kappa}{\mathfrak{p}}\right\} = 1$ and, as we see from the conclusion of the proof of Lemma 39 (p. 294), ε can always be chosen in such a way that a certain power of $\varepsilon\kappa$ with an exponent prime to l is congruent to $1 + \lambda$ modulo $\mathfrak{l}^2$. We consider now the Kummer field $k(\sqrt[l]{\varepsilon\kappa}, \zeta)$. By Theorem 148 (p. 227) the relative discriminant of this field with respect to $k(\zeta)$ has two prime factors $\mathfrak{q}$ and $\mathfrak{l}$. Since $\mathfrak{q}$ is a prime ideal of the second kind we deduce from Lemmas 36 and 37 that for every unit ξ in $k(\zeta)$ we have the equations

$$\left\{\frac{\xi, \varepsilon\kappa}{\mathfrak{l}}\right\} = \left\{\frac{\xi, \varepsilon}{\mathfrak{l}}\right\}\left\{\frac{\xi, \kappa}{\mathfrak{l}}\right\} = 1 \quad \text{and} \quad \left\{\frac{\xi}{\mathfrak{q}}\right\} = 1.$$

Consequently the number r of characters which determine the genus of an ideal in $k(\sqrt[l]{\varepsilon\kappa}, \zeta)$ is equal to 2. From Lemma 35 (p. 288) it follows that in $k(\sqrt[l]{\varepsilon\kappa}, \zeta)$ the number g of genera does not exceed l. Using Lemma 42 (p. 299) we determine a prime ideal $\mathfrak{r}$ in $k(\zeta)$ such that

$$\left\{\frac{\varepsilon\kappa}{\mathfrak{r}}\right\} = 1 \quad \text{and} \quad \left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\} \neq 1.$$

According to the first equation $\mathfrak{r}$ splits in $k(\sqrt[l]{\varepsilon\kappa}, \zeta)$. Let $\mathfrak{R}$ be a prime factor of $\mathfrak{r}$ in this field and ρ a primary number of $\mathfrak{r}$. Then the character set of the ideal $\mathfrak{R}$ in $k(\sqrt[l]{\varepsilon\kappa}, \zeta)$ consists of the two characters

$$\left\{\frac{\rho, \varepsilon\kappa}{\mathfrak{l}}\right\} \quad \text{and} \quad \left\{\frac{\rho, \varepsilon\kappa}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}. \tag{33.6}$$

Since the second character is not equal to 1 the ideals $\mathfrak{R}, \mathfrak{R}^2, \ldots, \mathfrak{R}^l$ determine distinct genera and, in view of the upper bound determined above for the number of genera, there can be no others. Using the first supplementary law proved in Sect. 159 we deduce that

$$\left\{\frac{\rho, \varepsilon\kappa}{\mathfrak{l}}\right\}\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\} = \left\{\frac{\rho, \varepsilon}{\mathfrak{l}}\right\}\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\} = \left\{\frac{\varepsilon}{\mathfrak{r}}\right\}\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\} = \left\{\frac{\varepsilon}{\mathfrak{r}}\right\}\left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\} = \left\{\frac{\varepsilon\kappa}{\mathfrak{r}}\right\} = 1,$$

i.e. the product of the two characters in (33.6) is 1. Since every ideal of $k(\sqrt[l]{\varepsilon\kappa}, \zeta)$ must belong to one of the l genera it follows that for every ideal

of $k(\sqrt[l]{\varepsilon\kappa},\zeta)$ the product of its two characters is always equal to 1. Since $\left\{\frac{\varepsilon\kappa}{\mathfrak{p}}\right\}=1$ the prime ideal $\mathfrak{p}$ splits in $k(\sqrt[l]{\varepsilon\kappa},\zeta)$; if $\mathfrak{P}$ is a prime factor of $\mathfrak{p}$ in this field then the two characters for $\mathfrak{P}$ are given by the symbols

$$\left\{\frac{\pi,\varepsilon\kappa}{\mathfrak{l}}\right\} \quad\text{and}\quad \left\{\frac{\pi,\varepsilon\kappa}{\mathfrak{q}}\right\}=\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}.$$

Using the first supplementary law proved in Sect. 159 we have

$$\left\{\frac{\pi,\varepsilon\kappa}{\mathfrak{l}}\right\}\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}=\left\{\frac{\pi,\varepsilon}{\mathfrak{l}}\right\}\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}=\left\{\frac{\varepsilon}{\mathfrak{p}}\right\}\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}=1$$

or

$$\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}=\left\{\frac{\varepsilon}{\mathfrak{p}}\right\}^{-1}=\left\{\frac{\kappa}{\mathfrak{p}}\right\}=\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\}.$$

That is to say, the reciprocity law holds for the two prime ideals $\mathfrak{p}$ and $\mathfrak{q}$.

Finally let $\mathfrak{q}$ and $\mathfrak{q}^*$ be two prime ideals of the second kind; let κ and κ^* be primary numbers for $\mathfrak{q}$ and $\mathfrak{q}^*$ respectively. We consider the Kummer field $k(\sqrt[l]{\kappa\kappa^*},\zeta)$. The numbers κ and κ^* are (as was shown in the proof of Lemma 37) congruent modulo $\mathfrak{l}^l$ to the l-th powers of certain integers in $k(\zeta)$; so the same holds for $\kappa\kappa^*$ and consequently, by Theorem 148 (p. 227), the relative discriminant of the field $k(\sqrt[l]{\kappa\kappa^*},\zeta)$ is not divisible by $\mathfrak{l}$. Thus the relative discriminant is divisible only by the prime ideals $\mathfrak{q}$ and $\mathfrak{q}^*$. Now for every unit ξ of $k(\zeta)$ we have

$$\left\{\frac{\xi,\kappa\kappa^*}{\mathfrak{q}}\right\}=\left\{\frac{\xi}{\mathfrak{q}}\right\}=1 \quad\text{and}\quad \left\{\frac{\xi,\kappa\kappa^*}{\mathfrak{q}^*}\right\}=\left\{\frac{\xi}{\mathfrak{q}^*}\right\}=1$$

and accordingly the number r of characters which determine the genus of an ideal in $k(\sqrt[l]{\kappa\kappa^*},\zeta)$ has the value 2. By Lemma 35 (p. 288) it follows that the number g of genera in the field $k(\sqrt[l]{\kappa\kappa^*},\zeta)$ does not exceed l. Using Theorem 152 (p. 254) we determine a prime ideal $\mathfrak{r}$ in $k(\zeta)$ such that

$$\left\{\frac{\kappa\kappa^*}{\mathfrak{r}}\right\}=1,\quad \left\{\frac{\zeta}{\mathfrak{r}}\right\}\neq 1 \quad\text{and}\quad \left\{\frac{\kappa}{\mathfrak{r}}\right\}\neq 1.$$

From the first equation it follows that $\mathfrak{r}$ splits in $k(\sqrt[l]{\kappa\kappa^*},\zeta)$; let $\mathfrak{R}$ be a prime factor of $\mathfrak{r}$ in this field and let ρ be a primary number for $\mathfrak{r}$. Then the character set of $\mathfrak{R}$ in $k(\sqrt[l]{\kappa\kappa^*},\zeta)$ consists of the two characters

$$\left.\begin{aligned}\left\{\frac{\rho,\kappa\kappa^*}{\mathfrak{q}}\right\}&=\left\{\frac{\rho}{\mathfrak{q}}\right\}=\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}\\ \left\{\frac{\rho,\kappa\kappa^*}{\mathfrak{q}^*}\right\}&=\left\{\frac{\rho}{\mathfrak{q}^*}\right\}=\left\{\frac{\mathfrak{r}}{\mathfrak{q}^*}\right\}\end{aligned}\right\} \tag{33.7}$$

Because $\left\{\frac{\kappa}{\mathfrak{r}}\right\}\neq 1$ it follows from Theorem 162 (p. 296) that the first character is distinct from 1. So the ideals $\mathfrak{R}, \mathfrak{R}^2, \ldots, \mathfrak{R}^l$ all determine different genera and there are, as we have already shown, no more than l genera. Since we have

$\left\{\frac{\xi}{\mathfrak{r}}\right\} \neq 1$ it follows that $\mathfrak{r}$ is a prime ideal of the first kind; so the reciprocity law holds for the prime ideals $\mathfrak{r}$ and $\mathfrak{q}$ and also for the prime ideals $\mathfrak{r}$ and $\mathfrak{q}^*$. Hence the product of the two characters (33.7) is

$$\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}\left\{\frac{\mathfrak{r}}{\mathfrak{q}^*}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\}\left\{\frac{\mathfrak{q}^*}{\mathfrak{r}}\right\} = \left\{\frac{\kappa\kappa^*}{\mathfrak{r}}\right\} = 1. \tag{33.8}$$

Since every ideal of $k(\sqrt[l]{\kappa\kappa^*}, \zeta)$ must belong to one of the l genera it follows from (33.8) that for every ideal the product of its two characters must be 1. Now the ideal $\mathfrak{q}$ is the l-th power of a prime ideal $\mathfrak{Q}$ in $k(\sqrt[l]{\kappa\kappa^*}, \zeta)$. The two characters of $\mathfrak{Q}$ in this field are thus

$$\left\{\frac{\kappa, \kappa\kappa^*}{\mathfrak{q}}\right\} = \left\{\frac{\kappa^*, \kappa\kappa^*}{\mathfrak{q}}\right\}^{-1} = \left\{\frac{\kappa^*}{\mathfrak{q}}\right\}^{-1} = \left\{\frac{\mathfrak{q}^*}{\mathfrak{q}}\right\}^{-1},$$

$$\left\{\frac{\kappa, \kappa\kappa^*}{\mathfrak{q}^*}\right\} = \left\{\frac{\kappa}{\mathfrak{q}^*}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{q}^*}\right\}$$

and since their product is 1 we obtain

$$\left\{\frac{\mathfrak{q}^*}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{q}^*}\right\}.$$

This establishes the reciprocity law for two prime ideals of the second kind and so completes the proof of the reciprocity law for any two prime ideals.

§161. Proof of the Second Supplementary Law for the Reciprocity Law

First let $\mathfrak{p}$ be a prime ideal of the first kind and π a primary number for $\mathfrak{p}$. We determine a unit ε in $k(\zeta)$ such that $\left\{\frac{\varepsilon\lambda}{\mathfrak{p}}\right\} = 1$ and then consider the Kummer field generated by $\sqrt[l]{\varepsilon\lambda}$ and ζ. Since $\left\{\frac{\varepsilon\lambda}{\mathfrak{p}}\right\} = 1$ it follows that $\mathfrak{p}$ splits in this field; let $\mathfrak{P}$ be a prime factor of $\mathfrak{p}$ in $k(\sqrt[l]{\varepsilon\lambda}, \zeta)$. We see that the character set of the prime ideal $\mathfrak{P}$ consists of the single character $\left\{\frac{\pi, \varepsilon\lambda}{\mathfrak{l}}\right\}$; since, by Lemma 35 (p. 288), there is only one genus (which must be the principal genus), this character must have the value 1. Since by Sect. 159 we have $\left\{\frac{\varepsilon}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \varepsilon}{\mathfrak{l}}\right\}$, it follows at once that $\left\{\frac{\lambda}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \lambda}{\mathfrak{l}}\right\}$.

Next let $\mathfrak{q}$ be a prime ideal of the second kind and let κ be a primary number for $\mathfrak{q}$. There are two cases to be considered, according as $\left\{\frac{\lambda}{\mathfrak{q}}\right\} = 1$ or $\neq 1$. In the first case it follows by considering the Kummer field $k(\sqrt[l]{\lambda}, \zeta)$ that we have $\left\{\frac{\kappa, \lambda}{\mathfrak{l}}\right\} = 1$ also. In the second case we use Theorem 152

(p. 254) to produce a prime ideal $\mathfrak{p}$ for which $\left\{\frac{\zeta}{\mathfrak{p}}\right\} = \left\{\frac{\kappa}{\mathfrak{p}}\right\}^{-1} \neq 1$. Then $\mathfrak{p}$ is certainly a prime ideal of the first kind and it follows by Theorem 162 (p. 296) that if π is a primary number for $\mathfrak{p}$ then $\left\{\frac{\pi}{\mathfrak{q}}\right\} \neq 1$; hence we can find a rational integer a such that $\left\{\frac{\lambda\pi^a}{\mathfrak{q}}\right\} = 1$. Consider now the Kummer field $k(\sqrt[l]{\lambda\pi^a}, \zeta)$. Then, since $\left\{\frac{\zeta, \lambda\pi^a}{\mathfrak{p}}\right\} = \left\{\frac{\zeta}{\mathfrak{p}}\right\}^a \neq 1$, the character set of an ideal of this field again consists only of a single character, which always takes the value 1. If we apply this fact to a prime factor $\mathfrak{Q}$ of $\mathfrak{q}$ in this field then it follows that $\left\{\frac{\zeta\kappa, \lambda\pi^a}{\mathfrak{l}}\right\} = \left\{\frac{\zeta}{\mathfrak{p}}\right\}^{-a}\left\{\frac{\kappa, \lambda}{\mathfrak{l}}\right\} = 1$; when we take into account the equation $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\}$ we obtain the result that $\left\{\frac{\lambda}{\mathfrak{q}}\right\} = \left\{\frac{\kappa, \lambda}{\mathfrak{l}}\right\}$.

The l-th power reciprocity law was first proved by Kummer. The new proof of the law which we have presented here differs from Kummer's proof above all in this, that Kummer began by obtaining the first supplementary law by an ingenious extension of the formulæ of cyclotomy (at the expense of considerable computation) and only then derived the reciprocity law for two prime ideals on the basis of the formulæ he had computed; in contrast to this the discussion we have given above draws the arguments for the reciprocity law and its two supplementary laws from a common source.

Among particular reciprocity laws which can be treated by the formulæ of cyclotomy we mention the reciprocity law for biquadratic residues (*Gauss* (3), *Eisenstein* (8, 9)), the reciprocity law for cubic residues (*Eisenstein* (5, 7), *Jacobi* (1)), the law for bicubic residues (*Gmeiner* (1, 2, 3)) and Jacobi's investigations concerning 5-th, 8-th and 12-th power residues (*Jacobi* (4)).

We should also mention in conclusion that Eisenstein has stated without proof an l-th power reciprocity law and moreover has also considered the case where the class number of the cyclotomic field of the l-th roots of unity is divisible by l (*Eisenstein* (1, 12)).

34. The Number of Genera in a Regular Kummer Field

§162. A Theorem on the Symbol $\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\}$

The most important problem in the theory of genera of a Kummer field is that of finding how many genera there actually are. We prove first a theorem which corresponds to Lemma 14 (p. 130) in the theory of quadratic fields.

Theorem 163. *If ν and μ are any nonzero integers of a regular cyclotomic field $k(\zeta)$ then*

$$\prod_{(\mathfrak{w})}\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\} = 1,$$

where the product on the left hand side is taken over all prime ideals $\mathfrak{w}$ of $k(\zeta)$.

Proof. Let h be the number of ideal classes in $k(\zeta)$ and h^* a positive rational integer such that $hh^* \equiv 1 \pmod{l}$. We set $\nu = \mathfrak{l}^a\mathfrak{p}_1\mathfrak{p}_2\cdots$ and $\mu = \mathfrak{l}^b\mathfrak{q}_1\mathfrak{q}_2\cdots$, where a and b are rational integer exponents and $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{q}_1, \mathfrak{q}_2, \ldots$ are prime ideals of $k(\zeta)$ distinct from $\mathfrak{l}$. Let $\pi_1, \pi_2, \ldots, \kappa_1, \kappa_2, \ldots$ be primary numbers for the prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{q}_1, \mathfrak{q}_2, \ldots$ respectively, chosen in such a way that

$$\pi_1 = \mathfrak{p}_1^{hh^*}, \pi_2 = \mathfrak{p}_2^{hh^*}, \ldots, \kappa_1 = \mathfrak{q}_1^{hh^*}, \kappa_2 = \mathfrak{q}_2^{hh^*}, \ldots.$$

If we set $\lambda = 1 - \zeta$ then we have two equations of the form

$$\nu = \varepsilon\lambda^{ahh^*}\pi_1\pi_2\cdots, \qquad \mu = \eta\lambda^{bhh^*}\kappa_1\kappa_2\cdots, \tag{34.1}$$

where ε and η are units of $k(\zeta)$. If $\mathfrak{w}$ is any prime ideal we have in general

$$\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\} = \left\{\frac{\nu^{hh^*},\mu^{hh^*}}{\mathfrak{w}}\right\}. \tag{34.2}$$

Now let $\mathfrak{p}$ and $\mathfrak{q}$ be two prime ideals distinct from one another and from $\mathfrak{l}$; let π and κ be primary numbers for $\mathfrak{p}$ and $\mathfrak{q}$ respectively. Let ε and η be any units in $k(\zeta)$. From Lemma 36 (p. 290) and Theorem 161 (p. 289) it is easy to deduce the formulæ

$$\left.\begin{array}{ll} \left\{\frac{\varepsilon,\eta}{\mathfrak{l}}\right\}=1, & \left\{\frac{\varepsilon,\lambda}{\mathfrak{l}}\right\}=1, \\ \left\{\frac{\varepsilon,\pi}{\mathfrak{l}}\right\}\left\{\frac{\varepsilon,\pi}{\mathfrak{p}}\right\}=1, & \left\{\frac{\pi,\kappa}{\mathfrak{p}}\right\}\left\{\frac{\pi,\kappa}{\mathfrak{q}}\right\}=1. \end{array}\right\} \tag{34.3}$$

If $\mathfrak{w}$ is a prime ideal distinct from $\mathfrak{l}$ which does not divide μ then, according to Theorem 148 (p. 227), the relative discriminant of the Kummer field $k(\sqrt[l]{\mu},\zeta)$ is prime to $\mathfrak{w}$; if $\mathfrak{w}$ is also prime to ν then, by Theorem 150 (p. 233), the number ν is a norm residue of $k(\sqrt[l]{\mu},\zeta)$ and hence, by Theorem 151 (p. 248), we have $\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\}=1$. This result together with (34.3) establishes the theorem in the case where each of the numbers ν, μ is either a unit or a power of λ or else a primary number for a prime ideal distinct from $\mathfrak{l}$. Then by (34.1) and (34.2), using the rules (29.9) and (29.12), we deduce Theorem 163 in general.

§163. The Fundamental Theorem on the Genera of a Regular Kummer Field

We are now in a position to state and prove the theorem for regular Kummer fields which corresponds to the fundamental Theorem 100 (p. 127) for quadratic fields. This theorem is as follows.

Theorem 164. *Let r be the number of characters which determine a genus in a regular Kummer field $K=k(\sqrt[l]{\mu},\zeta)$. Then a set of r l-th roots of unity is the character set of a genus of K if and only if the product of the r l-th roots of unity is* 1. *Thus the number of genera in K is l^{r-1}.*

Proof. Let h be the class number of the regular cyclotomic field $k(\zeta)$ and h^* a positive rational integer such that $hh^*\equiv 1 \pmod{l}$. Let $\mathfrak{l}_1,\ldots,\mathfrak{l}_r$ be the r prime ideal factors of the relative discriminant of K chosen as in Sect. 160. Let A be any ideal class in K, $\mathfrak{J}$ an ideal in the class A which is prime to $\mathfrak{l}=(1-\zeta)$ and to the relative discriminant of K; let $\bar{\nu}=(N_k(\mathfrak{J}))^{hh^*}$ be the integer of $k(\zeta)$ derived from $\mathfrak{J}$ according to Sect. 149 (p. 283) multiplied by a suitable unit factor so that

$$\chi_1(\mathfrak{J})=\left\{\frac{\bar{\nu},\mu}{\mathfrak{l}_1}\right\},\ldots,\chi_r(\mathfrak{J})=\left\{\frac{\bar{\nu},\mu}{\mathfrak{l}_r}\right\}$$

are the r characters which determine the genus of $\mathfrak{J}$. Let $\mathfrak{p}$ be an ideal of the cyclotomic field $k(\zeta)$, if there is one, which occurs as a factor of $\bar{\nu}$ to a power with exponent not divisible by l; then $\mathfrak{p}$ is certainly distinct from $\mathfrak{l}$ and prime to the relative discriminant of K. Since $N_k(\mathfrak{J})$ is the relative norm of an ideal it follows that $\mathfrak{p}$ must split in the field K. Consequently, applying Theorem

149 (p. 230), we deduce that for every such prime ideal $\mathfrak{p}$ we have $\left\{\frac{\mu}{\mathfrak{p}}\right\} = 1$ and hence also $\left\{\frac{\bar{\nu}, \mu}{\mathfrak{p}}\right\} = 1$. Referring to Theorem 163 (p. 305) we see that

$$\prod_{(\mathfrak{w})}\left\{\frac{\bar{\nu}, \mu}{\mathfrak{w}}\right\} = 1 \tag{34.4}$$

where $\mathfrak{w}$ runs over all prime ideals distinct from $\mathfrak{l}$ which divide the relative discriminant of K and also the prime ideal $\mathfrak{l}$. Further, if $\mathfrak{l}_{r+1}, \mathfrak{l}_{r+2}, \ldots, \mathfrak{l}_t$ are the prime ideals other than $\mathfrak{l}_1, \mathfrak{l}_2, \ldots, \mathfrak{l}_r$ which divide the relative discriminant, then by Sect. 149 we have

$$\left\{\frac{\bar{\nu}, \mu}{\mathfrak{l}_{r+1}}\right\} = 1, \ \left\{\frac{\bar{\nu}, \mu}{\mathfrak{l}_{r+2}}\right\} = 1, \ldots, \ \left\{\frac{\bar{\nu}, \mu}{\mathfrak{l}_t}\right\} = 1. \tag{34.5}$$

If the prime ideal $\mathfrak{l}$ divides the relative discriminant of the field K then it follows already from (34.4) that the product of all r characters is 1. If, on the other hand, $\mathfrak{l}$ does not divide the relative discriminant of K, then it follows from Theorem 150 (p. 233) that $\bar{\nu}$ is a norm residue of K modulo $\mathfrak{l}$ and hence, by Theorem 151 (p. 248), we have $\left\{\frac{\bar{\nu}, \mu}{\mathfrak{l}}\right\} = 1$. Thus we see from (34.4) and (34.5) that in this case also one part of Theorem 164 is established.

For the sake of brevity we shall prove the second part of the assertion of the theorem only in the case where the prime ideal $\mathfrak{l}$ does not divide the relative discriminant of the field K. Again we let $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$ be the t prime ideals of $k(\zeta)$ which divide the relative discriminant of K; let $\lambda_1, \ldots, \lambda_t$ be primary numbers for $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$ respectively. For $i = 1, \ldots, t$ let $\mathfrak{l}_1^{e_i}$ be the exact power of $\mathfrak{l}_i$ dividing μ and let e_1^* be a rational integer such that $e_i e_i^* \equiv 1 \pmod{l}$. Finally let $\gamma_1, \ldots, \gamma_r$ be any r l-th roots of unity such that $\gamma_1 \cdots \gamma_r = 1$; by Theorem 152 (p. 254) there exists a prime ideal $\mathfrak{p}$ of $k(\zeta)$ which does not divide μ and satisfies the equations

$$\left\{\frac{\lambda_1}{\mathfrak{p}}\right\}^m = \gamma_1^{e_1^*}, \ \left\{\frac{\lambda_2}{\mathfrak{p}}\right\}^m = \gamma_2^{e_2^*}, \ldots, \ \left\{\frac{\lambda_r}{\mathfrak{p}}\right\}^m = \gamma_r^{e_r^*}, \tag{34.6}$$

$$\left\{\frac{\lambda_{r+1}}{\mathfrak{p}}\right\}^m = 1, \ \left\{\frac{\lambda_{r+2}}{\mathfrak{p}}\right\}^m = 1, \ldots, \ \left\{\frac{\lambda_t}{\mathfrak{p}}\right\}^m = 1 \tag{34.7}$$

for some exponent m in the range $1, 2, \ldots, l-1$. If π is a primary number for $\mathfrak{p}$ it follows from (34.6), using Theorem 161 (p. 289), that

$$\left\{\frac{\pi^m, \mu}{\mathfrak{l}_i}\right\} = \left\{\frac{\pi, \mu}{\mathfrak{l}_i}\right\}^m = \left\{\frac{\pi}{\mathfrak{l}_i}\right\}^{me_i} = \left\{\frac{\lambda_i}{\mathfrak{p}}\right\}^{me_i} = \gamma_i \quad (i = 1, 2, \ldots, r). \tag{34.8}$$

Furthermore we deduce similarly from (34.7) that

$$\left\{\frac{\pi, \mu}{\mathfrak{l}_i}\right\} = \left\{\frac{\pi}{\mathfrak{l}_i}\right\}^{e_i} = \left\{\frac{\lambda_i}{\mathfrak{p}}\right\}^{e_i} = 1 \quad (i = r+1, r+2, \ldots, t). \tag{34.9}$$

Since $\gamma_1 \cdots \gamma_r = 1$ we deduce from (34.8) and (34.9) that

$$\prod_{(\mathfrak{w})} \left\{ \frac{\pi, \mu}{\mathfrak{w}} \right\} = 1 \tag{34.10}$$

if $\mathfrak{w}$ runs through all the prime ideals $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$. Now let $\mathfrak{m}$ be any prime ideal of $k(\zeta)$ distinct from $\mathfrak{p}$ and $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$. According to Theorem 150 (p. 233) the number π is a norm residue of the Kummer field K modulo $\mathfrak{m}$ and consequently, by Theorem 151 (p. 248), we have $\left\{ \frac{\pi, \mu}{\mathfrak{m}} \right\} = 1$. When we take account of this fact and (34.10) Theorem 163 (p. 305) implies that we must also have $\left\{ \frac{\pi, \mu}{\mathfrak{p}} \right\} = 1$, i.e. $\left\{ \frac{\mu}{\mathfrak{p}} \right\} = 1$. As a result of this last equation it follows, by Theorem 149 (p. 230), that the prime ideal $\mathfrak{p}$ splits in K as a product of l prime ideals. If $\mathfrak{P}$ is one of these then, as we see from (34.8) and (34.9), the ideal $\mathfrak{P}^m$ obviously has the prescribed roots of unity $\gamma_1, \ldots, \gamma_r$ as characters. Thus Theorem 164 is completely established in the case we are considering.

If $\mathfrak{l}$ divides the relative discriminant of K then in order to prove Theorem 164 we must make suitable modifications to the above argument – the appropriate changes are easily seen by analogy with the corresponding situation for quadratic fields (cf. pp. 144-145).

Kummer carried out his investigations in a certain order of the field $k(\sqrt[l]{\mu}, \zeta)$, not the totality of all the integers of this field. There the notion of genus requires certain modification. It was Kummer's great achievement to have stated and proved for the order he considered the results which we have formulated in Theorem 164 for the field K itself (*Kummer* (20)). Apart from the order considered by Kummer there are infinitely many other orders in K in which the theory could be developed with similar outcome.

§164. The Classes of the Principal Genus in a Regular Kummer Field

In this and the following section we present some important consequences of the fundamental Theorem 164 for the Kummer field $k(\sqrt[l]{\mu}, \zeta)$ which correspond to the theorems about quadratic fields developed in Sect. 71 and Sect. 72 and in Sect. 82.

Theorem 165. *The number g of genera in a regular Kummer field is equal to the number of ambig complexes.*

Proof. If t and n have the meaning described in Theorem 159 (p. 280) then, when we recall that, according to Theorem 164 (p. 306), we have $g = l^{r-1}$, it follows from Lemma 34 (p. 287) that $r - 1 \le t + n - \frac{1}{2}(l+1)$; since, by

Lemma 33 (p. 285), we have on the other hand that $t+n-\frac{1}{2}(l+1) \leq r-1$, it follows that

$$r-1 = t+n-\tfrac{1}{2}(l+1).$$

We thus see that the number a of ambig complexes determined in the proof of Lemma 34 (p. 287) must be l^{r-1} and hence we have $a = g$.

Theorem 166. *Every complex in the principal genus of a regular Kummer field K is the $(1-S)$-th symbolic power of a complex in K, i.e. every class in the principal genus is the product of the $(1-S)$-th symbolic power of a class by a class which contains ideals of $k(\zeta)$.*

Proof. In the proof of Lemma 34 (p. 287) we obtained the equation $af' = gf$ where a is the number of ambig complexes, f' the number of complexes which are $(1-S)$-th symbolic powers of complexes, g is the number of genera and f is the number of complexes in the principal genus. Since we have proved in Theorem 165 that $a = g$ it follows that $f' = f$ and so every complex in the principal genus is the $(1-S)$-th power of a complex.

§165. Theorem on the Relative Norms of Numbers in a Regular Kummer Field

Theorem 167. *Let ν and μ be integers of the regular cyclotomic field $k(\zeta)$ such that μ is not the l-th power of an integer in $k(\zeta)$. If for every prime ideal $\mathfrak{w}$ of $k(\zeta)$ we have*

$$\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\} = 1$$

then the number ν is the relative norm of an integer or fraction A of the Kummer field $K = k(\sqrt[l]{\mu}, \zeta)$.

Proof. We prove this result first in the case where ν is a unit in $k(\zeta)$. Again let n and t have the same meaning for the field $k(\sqrt[l]{\mu}, \zeta)$ as in Theorem 159 (p. 280). In the proof of Theorem 159 it was shown that $r-1 = t+n-\frac{1}{2}(l+1)$, whence $n = \frac{1}{2}(l-1)-t+r$. We consider on the other hand the $r^* = t-r$ units $\varepsilon_1, \ldots, \varepsilon_{r^*}$ which were determined in Sect. 149 (pp. 283-284). According to the equations (32.19) (p. 284) a product of powers of these r^* units can be the l-th power of a unit of $k(\zeta)$ only if the exponents of the powers are all divisible by l. Since the set of all units in $k(\zeta)$ forms a unit bundle of degree $\frac{1}{2}(l-1)$ it follows that there must be a further $\frac{1}{2}(l-1)-r^*$ units ε_{r^*+1}, $\varepsilon_{r^*+2}, \ldots, \varepsilon_{\frac{1}{2}(l-1)}$ in $k(\zeta)$ such that every unit ξ in $k(\zeta)$ can be expressed in the form

$$\xi = \varepsilon_1^{x_1}\varepsilon_2^{x_2}\cdots\varepsilon_{\frac{1}{2}(l-1)}^{x_{\frac{1}{2}(l-1)}}\varepsilon^l$$

where $x_1, x_2, \ldots, x_{\frac{1}{2}(l-1)}$ are rational integer exponents and ε is a suitably chosen unit in $k(\zeta)$. Let us set in general

$$\left\{\frac{\varepsilon_u, \mu}{\mathfrak{l}_{t-v+1}}\right\} = \zeta^{e_{uv}} \qquad (u = 1, 2, \ldots, \tfrac{1}{2}(l-1); v = 1, 2, \ldots, r^*).$$

Then the r^* equations

$$\left\{\frac{\xi, \mu}{\mathfrak{l}_t}\right\} = 1, \left\{\frac{\xi, \mu}{\mathfrak{l}_{t-1}}\right\} = 1, \ldots, \left\{\frac{\xi, \mu}{\mathfrak{l}_{t-r^*+1}}\right\} = 1 \tag{34.11}$$

lead to the following r^* linear congruences for the exponents $x_1, x_2, \ldots, x_{\frac{1}{2}(l-1)}$:

$$\left.\begin{array}{l} e_{11}x_1 + \cdots + e_{\frac{1}{2}(l-1),1}x_{\frac{1}{2}(l-1)} \equiv 0 \\ \cdots\cdots \\ e_{1r^*}x_1 + \cdots + e_{\frac{1}{2}(l-1),r^*}x_{\frac{1}{2}(l-1)} \equiv 0. \end{array}\right\} \pmod{l} \tag{34.12}$$

According to (32.19) (p. 284) we have

$$\left.\begin{array}{llllll} e_{11} \equiv 1, & e_{21} \equiv 0, & e_{31} \equiv 0, & \ldots, & e_{r^*1} \equiv 0 \\ & e_{22} \equiv 1, & e_{32} \equiv 0, & \ldots, & e_{r^*2} \equiv 0 \\ & & e_{33} \equiv 1, & \ldots, & e_{r^*3} \equiv 0 \\ & & & \ldots & \\ & & & & e_{r^*r^*} \equiv 1 \end{array}\right\} \pmod{l}$$

and hence the r^* linear congruences (34.12) are independent. It follows that all the units ξ which satisfy conditions (34.11) form a unit bundle of degree

$$\tfrac{1}{2}(l-1) - r^* = \tfrac{1}{2}(l-1) - t + r.$$

We established at the beginning of this proof that the degree n of the bundle of all units in $k(\zeta)$ which are relative norms of units or fractions in K has this same value $\frac{1}{2}(l-1) - t + r$. Since every unit in $k(\zeta)$ which is the relative norm of a unit or a fraction in K is obviously a norm residue of K modulo $\mathfrak{l}$ and hence, by Theorem 151 (p. 248), must satisfy the equations (34.11), it follows that every unit of the bundle considered at the beginning also belongs to the second unit bundle. Since both bundles have the same degree they must be identical. By hypothesis the unit ν under consideration satisfies the conditions (34.11) and hence belongs to the second unit bundle; hence, by what we have just proved, ν belongs also to the first unit bundle, i.e. ν is the relative norm of a unit or a fraction in K.

Now let ν be any integer in K which satisfies the condition of Theorem 167. We consider the prime ideals of the field K which divide ν. Set $\lambda = 1 - \zeta$ and $\mathfrak{l} = (\lambda)$. If the prime ideal $\mathfrak{l}$ of the field $k(\zeta)$ occurs as a factor of ν to a power whose exponent b is not divisible by l and if, furthermore $\mathfrak{l}$ does not divide the relative discriminant of K then, using the results at the end of Sect. 133 on p. 251, we see that we have

$$\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}=\left\{\frac{\lambda^b,\mu}{\mathfrak{l}}\right\}=\left\{\frac{\mu}{\mathfrak{l}}\right\}^{-b};$$

then, as a consequence of the equation

$$\left\{\frac{\mu}{\mathfrak{l}}\right\}=1$$

which we derive from this, we deduce from Theorem 149 (p. 230) that $\mathfrak{l}$ splits in K as a product of l prime ideals. Let $\mathfrak{L}$ be one of these; then we have $N_k(\mathfrak{L})=\mathfrak{l}$.

Next let $\mathfrak{p}$ be a prime ideal of the cyclotomic field $k(\zeta)$ distinct from $\mathfrak{l}$. Suppose that $\mathfrak{p}$ occurs as a factor of ν to a power whose exponent b is not divisible by l; on the other hand suppose that the exponent a of the power to which $\mathfrak{p}$ divides μ is divisible by l. Then, by definition of the symbol, we have

$$\left\{\frac{\nu,\mu}{\mathfrak{p}}\right\}=\left\{\frac{\mu^b}{\mathfrak{p}}\right\}^{-1}$$

and hence, according to the hypothesis of Theorem 167, we have $\left\{\frac{\mu}{\mathfrak{p}}\right\}=1$. From Theorem 149 (p. 230) we deduce that $\mathfrak{p}$ splits in K as a product of l prime ideals. If $\mathfrak{P}$ is one of these ideals we have $\mathfrak{p}=N_k(\mathfrak{P})$.

Finally, the prime ideals of $k(\zeta)$ which divide the relative discriminant of K are all l-th powers of prime ideals in K and hence relative norms of ideals of K. When all these facts are taken together it follows that ν must be the relative norm of an ideal $\mathfrak{H}$ in K, i.e. that $\nu=N_k(\mathfrak{H})$.

According to the hypothesis of Theorem 167 we see further that $\mathfrak{H}$ belongs to the principal genus of K and hence, by Theorem 166 (p. 309), we can write

$$\mathfrak{H}\sim\mathfrak{i}\mathfrak{J}^{1-S}$$

where $\mathfrak{i}$ is an ideal in $k(\zeta)$ and $\mathfrak{J}$ is an ideal in K. If h is the number of ideal classes in $k(\zeta)$ we have $\mathfrak{i}^h\sim 1$ and consequently $\mathsf{A}=\left(\frac{\mathfrak{H}}{\mathfrak{J}^{1-S}}\right)^h$ must be an integer or fraction in the field K; for the relative norm of this number A we clearly have $N_k(\mathsf{A})=\varepsilon\nu^h$ where ε is a unit in $k(\zeta)$. From this equation it follows by Theorem 151 (p. 248) that for every prime ideal $\mathfrak{w}$ in $k(\zeta)$ we have $\left\{\frac{\varepsilon\nu^h,\mu}{\mathfrak{w}}\right\}=1$ and hence also $\left\{\frac{\varepsilon,\mu}{\mathfrak{w}}\right\}=1$. Now in the first part of this proof it was shown that under this condition ε must be the relative norm of a number in K; we set $\varepsilon=N_k(\mathsf{H})$ where H is in K. If b and e are rational integers such that $bh+el=1$ it follows that

$$\nu=N_k(\mathsf{A}^b\mathsf{H}^{-b}\nu^e),$$

and this completes the proof of Theorem 167.

In this proof we can on both occasions restrict the application of Theorem 151 to the case where $\mathfrak{w} \neq \mathfrak{l}$ since then, by Theorem 163 (p. 305), the assertion follows also for $\mathfrak{w} = \mathfrak{l}$.

With this we have succeeded in carrying over to regular Kummer fields all the properties which were already stated and proved by Gauss for quadratic fields.

35. New Foundation of the Theory of Regular Kummer Fields

§166. Essential Properties of the Units of a Regular Cyclotomic Field

We have seen how important a role the symbol $\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}$ plays in the theory of Kummer fields. The definition of this symbol in Sect. 131 and the derivation of its properties in Sect. 131 to Sect. 133 were intimately connected with the logarithmic derivative (introduced by Kummer) of the function $\omega(x)$ associated with a number ω congruent to 1 modulo $\mathfrak{l}$. The computations involving the symbol $\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}$ in a Kummer field which were carried out in Sect. 131 to Sect. 133 correspond precisely to the considerations presented in Sect. 64 for the symbol $\left(\frac{n,m}{2}\right)$ in a quadratic field. Although we have already succeeded in reducing the computational machinery invented by Kummer to modest dimensions, it still seems to me necessary, especially for the future development of the theory, to investigate whether it might not be possible to lay a foundation for the theory of Kummer fields completely lacking any computation. In this chapter I indicate briefly the way to do this.

First of all it is easy to deduce the properties of the units of a regular cyclotomic field which will be needed later on without any calculation and without introducing the Bernoulli numbers. For Theorem 156 we call to mind the second of the proofs given on p. 266.

We can then deduce Theorem 155 (p. 264) from Theorem 156 as follows. We let $\varepsilon_1, \ldots, \varepsilon_{l^*}$ be any fundamental set of l^* units of the field $k(\zeta)$; then we determine positive exponents $e_1, \ldots, e_{l^*}$ and rational integers $a_1, \ldots, a_{l^*}$ $b_1, \ldots, b_{l^*}$ prime to l such that the congruences

$$\begin{aligned} \varepsilon_1 &\equiv a_1 + b_1\lambda^{e_1} \quad (\bmod\ \mathfrak{l}^{e_1+1}) \\ &\cdots\cdots \\ \varepsilon_{l^*} &\equiv a_{l^*} + b_{l^*}\lambda^{e_{l^*}} \quad (\bmod\ \mathfrak{l}^{e_{l^*}+1}) \end{aligned}$$

are satisfied. We suppose that e_1 is the least among the exponents $e_1, \ldots, e_{l^*}$. Then it is easy to see that the $l^* - 1$ units $\varepsilon_2, \ldots, \varepsilon_{l^*}$ can be multiplied by powers of ε_1 in such a way that the $l^* - 1$ products $\varepsilon_2', \ldots, \varepsilon_{l^*}'$ so obtained satisfy the congruences

$$\varepsilon_2' = \varepsilon_2 \varepsilon_1^{f_2} \equiv a_2' + b_2' \lambda^{e_2'} \pmod{\mathfrak{l}^{e_2'+1}}$$
$$\cdots\cdots$$
$$\varepsilon_{l^*}' = \varepsilon_{l^*} \varepsilon_1^{f_{l^*}} \equiv a_{l^*}' + b_{l^*}' \lambda^{e_{l^*}'} \pmod{\mathfrak{l}^{e_{l^*}'+1}}$$

where $a_2', \ldots, a_{l^*}', b_2', \ldots, b_{l^*}'$ are rational integers prime to l and the exponents $e_2', \ldots, e_{l^*}'$ are all greater than e_1. The units $\varepsilon_1, \varepsilon_2', \varepsilon_3', \ldots, \varepsilon_{l^*}'$ form a fundamental set of units for $k(\zeta)$. Now suppose that e_2' is the least among the exponents $e_2', \ldots, e_{l^*}'$. Then it is again possible to multiply the units ε_3', $\ldots, \varepsilon_{l^*}'$ by powers of ε_2' so that the $l^* - 2$ products $\varepsilon_3'', \ldots, \varepsilon_{l^*}''$ satisfy the congruences

$$\varepsilon_3'' = \varepsilon_3' \varepsilon_2'^{f_3'} \equiv a_3'' + b_3'' \lambda^{e_3''} \pmod{\mathfrak{l}^{e_3''+1}}$$
$$\cdots\cdots$$
$$\varepsilon_{l^*}'' = \varepsilon_{l^*}' \varepsilon_2'^{f_{l^*}'} \equiv a_{l^*}'' + b_{l^*}'' \lambda^{e_{l^*}''} \pmod{\mathfrak{l}^{e_{l^*}''+1}}$$

where $a_3'', \ldots, a_{l^*}'', b_3'', \ldots, b_{l^*}$ are rational integers prime to l and the exponents $e_3'', \ldots, e_{l^*}''$ are all greater than e_2'. The units $\varepsilon_1, \varepsilon_2', \varepsilon_3'', \varepsilon_4'', \ldots, \varepsilon_{l^*}''$ again form a fundamental set of units for $k(\zeta)$. Proceeding in this way we obtain eventually a fundamental set $\varepsilon_1, \varepsilon_2', \varepsilon_3'', \ldots, \varepsilon_{l^*}^{(l^*-1)}$ of units in $k(\zeta)$ which satisfy the congruences

$$\begin{aligned}
\varepsilon_1 &\equiv a_1 + b_1 \lambda^{e_1} && \pmod{\mathfrak{l}^{e_1+1}} \\
\varepsilon_2' &\equiv a_2' + b_2' \lambda^{e_2'} && \pmod{\mathfrak{l}^{e_2'+1}} \\
\varepsilon_3'' &\equiv a_3'' + b_3'' \lambda^{e_3''} && \pmod{\mathfrak{l}^{e_3''+1}} \\
&\cdots\cdots \\
\varepsilon_{l^*}^{(l^*-1)} &\equiv a_{l^*}^{(l^*-1)} + b_{l^*}^{(l^*-1)} \lambda^{e_{l^*}^{(l^*-1)}} && \pmod{\mathfrak{l}^{e_{l^*}^{(l^*-1)}+1}}
\end{aligned}$$

where $a_1, \ldots, a_{l^*}^{(l^*-1)}, b_1, \ldots, b_{l^*}^{(l^*-1)}$ are rational integers prime to l and the exponents $e_1, \ldots, e_{l^*}^{(l^*-1)}$ satisfy the chain of inequalities

$$e_1 < e_2' < e_3'' < \cdots < e_{l^*}^{(l^*-1)}. \tag{35.1}$$

Since the units under consideration are all real the exponents $e_1, e_2', e_3'', \ldots, e_{l^*}^{(l^*-1)}$ are all even. If we had

$$e_{l^*}^{(l^*-1)} \geq l - 1$$

then (by Theorem 156) $\varepsilon_{l^*}^{(l^*-1)}$ would be the l-th power of a unit η in $k(\zeta)$. If we express η by means of the units $\zeta, \varepsilon_1, \varepsilon_2', \ldots, \varepsilon_{l^*}^{(l^*-1)}$ in the form

$$\eta = \zeta^u \varepsilon_1^{u_1} (\varepsilon_2')^{u_2} \cdots (\varepsilon_{l^*}^{(l^*-1)})^{u_{l^*}},$$

where $u, u_1, u_2, \ldots, u_{l^*}$ are rational integer exponents, and raise this equation to the l-th power then we obtain a relation between the l^* units $\varepsilon_1, \varepsilon_2', \ldots,$

$\varepsilon_{l^*}^{(l^*-1)}$ with exponents which are not all zero; this contradicts the fact that $\varepsilon_1, \varepsilon_2', \ldots, \varepsilon_{l^*}^{(l^*-1)}$ form a fundamental set of units for $k(\zeta)$. It follows that

$$e_{l^*}^{(l^*-1)} < l - 1.$$

Hence, examining the inequalities (35.1), we see that we must have

$$e_1 = 2, e_2' = 4, e_3'' = 6, \ldots, e_{l^*}^{(l^*-1)} = l - 3.$$

This fact allows us to conclude at once that there exist units $\bar{\varepsilon}_1, \ldots, \bar{\varepsilon}_{l^*}$ with the property required by Theorem 155 (p. 264).

Theorem 157 (p. 266) follows from Theorem 155 as in Sect. 142.

§167. Proof of a Property of Primary Numbers for Prime Ideals of the Second Kind

We take as basis for our discussion the definition of the symbol $\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\}$ given in Sect. 131 for a prime ideal $\mathfrak{w} \neq \mathfrak{l}$, leaving aside for the present a definition of the symbol $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$; accordingly we make use of Theorems 150 (p. 233) and 151 (p. 248) only for $\mathfrak{w} \neq \mathfrak{l}$. Theorems 158 (p. 273) and 159 (p. 280) then follow immediately for the Kummer field $k(\sqrt[l]{\mu}, \zeta)$ as shown earlier, provided we make the restrictive assumption that the relative discriminant of $k(\sqrt[l]{\mu}, \zeta)$ with respect to $k(\zeta)$ is prime to $\mathfrak{l}$. Under the same restriction we obtain, without using the symbol $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$, the notion of the character of an ideal in $k(\sqrt[l]{\mu}, \zeta)$, the classification of the ideal classes of a Kummer field into genera and the validity of Lemmas 33 (p. 285), 34 (p. 287) and 35 (p. 288). Then we can prove first the following lemma.

Lemma 43. *Every primary number κ for a prime ideal $\mathfrak{q}$ of the second kind is congruent modulo $\mathfrak{l}^l$ to the l-th power of an integer in $k(\zeta)$.*

Proof. Let $\varepsilon_1, \ldots, \varepsilon_{l^*}$ be the $l^* = \frac{1}{2}(l-3)$ fundamental units of the field $k(\zeta)$ determined in Sect. 166 (denoted there by $\varepsilon_1, \varepsilon_2', \ldots, \varepsilon_{l^*}^{(l^*-1)}$). Let $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_{l^*}$ be prime ideals of $k(\zeta)$ distinct from $\mathfrak{l}$ such that

$$\left.\begin{array}{lllll} \left\{\frac{\zeta}{\mathfrak{p}}\right\} = \zeta^*, & \left\{\frac{\varepsilon_1}{\mathfrak{p}}\right\} = 1, & \left\{\frac{\varepsilon_2}{\mathfrak{p}}\right\} = 1, & \ldots, & \left\{\frac{\varepsilon_{l^*}}{\mathfrak{p}}\right\} = 1, \\ \left\{\frac{\zeta}{\mathfrak{p}_1}\right\} = 1, & \left\{\frac{\varepsilon_1}{\mathfrak{p}_1}\right\} = \zeta_1, & \left\{\frac{\varepsilon_2}{\mathfrak{p}_1}\right\} = 1, & \ldots, & \left\{\frac{\varepsilon_{l^*}}{\mathfrak{p}_1}\right\} = 1, \\ & \cdots & \cdots & \cdots & \\ \left\{\frac{\zeta}{\mathfrak{p}_{l^*}}\right\} = 1, & \left\{\frac{\varepsilon_1}{\mathfrak{p}_{l^*}}\right\} = 1, & \left\{\frac{\varepsilon_2}{\mathfrak{p}_{l^*}}\right\} = 1, & \ldots, & \left\{\frac{\varepsilon_{l^*}}{\mathfrak{p}_{l^*}}\right\} = \zeta_{l^*}, \end{array}\right\} \quad (35.2)$$

where $\zeta^*, \zeta_1, \ldots, \zeta_{l^*}$ are any l-th roots of unity distinct from 1. The existence of such prime ideals follows from Theorem 152 (p. 254); if we refer back to the proof of this theorem we see that not only the number but also the sum of the reciprocals of the norms of all the prime ideals $\mathfrak{r}$ with the properties given there are infinite; accordingly, as is clear from consideration of the proof of Theorem 83 (p. 95), we may suppose in the present situation that the prime ideals $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_{l^*}$ are all of degree 1. Furthermore we can suppose that the rational prime numbers divisible by $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_{l^*}$ are all distinct. Let $\pi, \pi_1, \ldots, \pi_{l^*}$ be primary numbers for $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_{l^*}$ respectively.

We now examine the possibility that there are $l^* + 1$ integer exponents $u, u_1, \ldots, u_{l^*}$, not all divisible by l, for which the expression $\alpha = \pi^u \pi_1^{u_1} \cdots \pi_{l^*}^{u_{l^*}}$ is congruent modulo $\mathfrak{l}^l$ to the l-th power of an integer in $k(\zeta)$. By Theorem 148 (p. 227) the relative discriminant of the Kummer field $k(\sqrt[l]{\alpha}, \zeta)$ is divisible by a certain number t of the prime ideals $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_{l^*}$ but not by the prime ideal $\mathfrak{l}$. On the other hand it follows from (35.2) with the help of Theorem 151 (p. 248) that the degree m of the unit bundle consisting of the units of $k(\zeta)$ which are relative norms of units in $k(\sqrt[l]{\alpha}, \zeta)$ is no greater than $\frac{1}{2}(l-1) - t$; thus for the Kummer field $k(\sqrt[l]{\alpha}, \zeta)$ we would have

$$m \leq \tfrac{1}{2}(l-1) - t, \quad \text{i.e.} \quad t + m - \tfrac{1}{2}(l-1) \leq 0$$

which, according to Theorem 158 (p. 273) cannot be the case. Hence the possibility described above cannot occur and so if the exponents $u, u_1, \ldots, u_{l^*}$ are all prime to l the number $\pi^u \pi_1^{u_1} \cdots \pi_{l^*}^{u_{l^*}}$ cannot be congruent modulo $\mathfrak{l}^l$ to the l-th power of an integer in $k(\zeta)$.

Let κ be a primary number for the prime ideal $\mathfrak{q}$. We deduce from the proof of Theorem 157 (p. 266) that there are precisely $(l-1)l^{l-3}/l^{l^*}$ primary numbers mutually incongruent modulo $\mathfrak{l}^{l-1}$ and hence $(l-1)l^{l^*+1}$ mutually incongruent modulo $\mathfrak{l}^l$; on the other hand the l-th power of a number in $k(\zeta)$ which is prime to $\mathfrak{l}$ is always congruent modulo $\mathfrak{l}^l$ to the l-th power of one of the $l-1$ numbers $1, 2, \ldots, l-1$. From the facts we have just obtained it follows that it must always be possible to determine the exponents $u, u_1, \ldots, u_{l^*}$ in such a way that the expression $\mu = \pi^u \pi_1^{u_1} \cdots \pi_{l^*}^{u_{l^*}} \kappa$ is congruent modulo $\mathfrak{l}^l$ to the l-th power of an integer of $k(\zeta)$; if $u, u_1, \ldots, u_{l^*}$ are obtained in this way then we write $\alpha = \pi^u \pi_1^{u_1} \cdots \pi_{l^*}^{u_{l^*}}$, so that $\mu = \alpha\kappa$. Consider now the possibility that a certain *positive* number a of the exponents $u, u_1, \ldots, u_{l^*}$ are prime to l while the remaining $\frac{1}{2}(l-1) - a$ are divisible by l. Then by (35.2) we see that for the Kummer field $k(\sqrt[l]{\mu}, \zeta)$ we have (using the notation of Sect. 149) $t = a + 1$, $r^* = a$, $r = t - r^* = 1$ and hence, by Lemma 35 (p. 288), all ideal classes of the field $k(\sqrt[l]{\mu}, \zeta)$ belong to the principal genus. This implies at once that if $\mathfrak{r}$ is any prime ideal of $k(\zeta)$ with the property $\left\{\frac{\mu}{\mathfrak{r}}\right\} = 1$ and ρ is a primary number for $\mathfrak{r}$ then, by suitable choice of the unit ξ, the character set of the number $\xi\rho$ in the field $k(\sqrt[l]{\mu}, \zeta)$ consists entirely of units $+1$; hence in particular

$$\left\{\frac{\xi\rho,\mu}{\mathfrak{q}}\right\} = \left\{\frac{\xi\rho}{\mathfrak{q}}\right\} = 1$$

and since $\mathfrak{q}$ is a prime ideal of the second kind it follows that $\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\} = 1$.

Next we denote the ideals distinct from $\mathfrak{q}$ and conjugate to it by $\mathfrak{q}'$, $\mathfrak{q}''$, ... and the automorphisms in the group of $k(\zeta)$ which transform $\mathfrak{q}$ into $\mathfrak{q}'$, $\mathfrak{q}''$, ... by s', s'', ... respectively. If h and h^* have the same meaning as in Sect. 149 and q is the rational prime divisible by $\mathfrak{q}$ then, just as in Sect. 158, when we take account of the remark after Theorem 157 (p. 266), we have

$$\kappa(s'\kappa)(s''\kappa)\cdots = \varepsilon^l q^{hh^*}$$

where ε is a unit in $k(\zeta)$. According to our assumption about the exponents $u, u_1, \ldots, u_{l^*}$ and since the prime ideals $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_{l^*}$ are of degree 1 and divide distinct rational primes we can conclude from Theorem 152 (p. 258) that there is a prime ideal $\mathfrak{r}$ of $k(\zeta)$ with the properties

$$\left.\begin{array}{ll} \left\{\frac{\alpha}{\mathfrak{r}}\right\} = (\zeta^*)^{-1}, & \left\{\frac{\kappa}{\mathfrak{r}}\right\} = \zeta^*, \\ \left\{\frac{s'\alpha}{\mathfrak{r}}\right\} = 1, & \left\{\frac{s'\kappa}{\mathfrak{r}}\right\} = 1, \\ \left\{\frac{s''\alpha}{\mathfrak{r}}\right\} = 1, & \left\{\frac{s''\kappa}{\mathfrak{r}}\right\} = 1, \\ \cdots & \cdots \end{array}\right\} \qquad (35.3)$$

where ζ^* is any l-th root of unity distinct from 1. The equations (35.3) give at once

$$\left\{\frac{\mu}{\mathfrak{r}}\right\} = 1, \ \left\{\frac{s'\mu}{\mathfrak{r}}\right\} = 1, \ \left\{\frac{s''\mu}{\mathfrak{r}}\right\} = 1, \ldots, \qquad (35.4)$$

$$\left\{\frac{\kappa\cdot s'\kappa\cdot s''\kappa\cdots}{\mathfrak{r}}\right\} = \left\{\frac{q}{\mathfrak{r}}\right\} = \zeta^*; \qquad (35.5)$$

from the first of the equations (35.4) it follows by what was previously proved that $\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\} = 1$ and similarly the remaining equations in (35.4) lead to the relations $\left\{\frac{\mathfrak{r}}{\mathfrak{q}'}\right\} = 1$, $\left\{\frac{\mathfrak{r}}{\mathfrak{q}''}\right\} = 1$, ... Multiplying these relations we obtain $\left\{\frac{\mathfrak{r}}{q}\right\} = 1$ which, according to Theorem 140 (p. 202) contradicts equation (35.5). It follows that the possibility we are considering in relation to the exponents $u, u_1, \ldots, u_{l^*}$ cannot in fact occur, i.e. these exponents as determined above must all be divisible by l and hence α is the l-th power of an integer in $k(\zeta)$. From this it follows that κ is congruent modulo $\mathfrak{l}^l$ to the l-th power of an integer in $k(\zeta)$ and so the proof of Lemma 43 is complete.

§168. Proof of the Reciprocity Law Where One of the Two Prime Ideals is of the Second Kind

Now we prove successively the separate parts of the l-th power reciprocity law as follows.

Lemma 44. *Let* $\mathfrak{q}$ *be a prime ideal of the second kind and* $\mathfrak{r}$ *a prime ideal of the first or second kind in* $k(\zeta)$. *If* $\left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\} = 1$ *then* $\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\} = 1$ *also.*

Proof. Let κ and ρ be primary numbers for $\mathfrak{q}$ and $\mathfrak{r}$ respectively. Referring to Lemma 43 (p. 315) we see that by Theorem 148 (p. 227) the relative discriminant of the field $k(\sqrt[l]{\kappa}, \zeta)$ has only the single prime factor $\mathfrak{q}$; hence, according to Lemma 35 (p. 288), all ideals of this field belong to the principal genus. Since $\left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\} = 1$ the prime ideal $\mathfrak{r}$ splits in the field $k(\sqrt[l]{\kappa}, \zeta)$ as a product of l prime ideals; the character of any one of these prime ideals has the value

$$\left\{\frac{\rho, \kappa}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\} = 1;$$

this completes the proof of Lemma 44.

Lemma 45. *If* $\mathfrak{q}$ *and* $\mathfrak{q}_1$ *are any two prime ideals of the second kind in* $k(\zeta)$ *then* $\left\{\frac{\mathfrak{q}}{\mathfrak{q}_1}\right\} = \left\{\frac{\mathfrak{q}_1}{\mathfrak{q}}\right\}$.

Proof. If $\left\{\frac{\mathfrak{q}}{\mathfrak{q}_1}\right\} = 1$ then the assertion of the lemma follows at once from Lemma 44.

We now consider the case in which $\left\{\frac{\mathfrak{q}}{\mathfrak{q}_1}\right\} \neq 1$. Let κ and κ_1 be primary numbers for $\mathfrak{q}$ and $\mathfrak{q}_1$ respectively; let $\mathfrak{q}', \mathfrak{q}'', \ldots$ be the prime ideals distinct from $\mathfrak{q}$ which are conjugate to it and let $\kappa', \kappa'', \ldots$ be the primary numbers for $\mathfrak{q}', \mathfrak{q}'', \ldots$ respectively conjugate to κ. Similarly let $\mathfrak{q}_1', \mathfrak{q}_1'', \ldots$ be the prime ideals distinct from $\mathfrak{q}_1$ which are conjugate to it and $\kappa_1', \kappa_1'', \ldots$ the primary numbers for $\mathfrak{q}_1', \mathfrak{q}_1'', \ldots$ respectively conjugate to κ_1. Finally let q be the rational prime number divisible by $\mathfrak{q}$; then we have $\kappa\kappa'\kappa'' \cdots = \varepsilon^l q^{hh^*}$ where ε is a unit in $k(\zeta)$. By Theorem 152 (p. 254) there is a prime ideal $\mathfrak{r}$ for which

$$\left\{\frac{\kappa}{\mathfrak{r}}\right\} = \zeta^*, \ \left\{\frac{\kappa'}{\mathfrak{r}}\right\} = 1, \ \left\{\frac{\kappa''}{\mathfrak{r}}\right\} = 1, \ldots, \tag{35.6}$$

$$\left\{\frac{\kappa_1}{\mathfrak{r}}\right\} = \zeta^*, \ \left\{\frac{\kappa_1'}{\mathfrak{r}}\right\} = 1, \ \left\{\frac{\kappa_1''}{\mathfrak{r}}\right\} = 1, \ldots, \tag{35.7}$$

$$\left\{\frac{\zeta}{\mathfrak{r}}\right\} = 1, \ \left\{\frac{\varepsilon_1}{\mathfrak{r}}\right\} = 1, \ \left\{\frac{\varepsilon_2}{\mathfrak{r}}\right\} = 1, \ldots, \ \left\{\frac{\varepsilon_{l^*}}{\mathfrak{r}}\right\} = 1, \tag{35.8}$$

where ζ^* is any l-th root of unity distinct from 1 and $\varepsilon_1, \ldots, \varepsilon_{l^*}$ are the l^* units determined in Sect. 166 (denoted there by $\varepsilon_1, \varepsilon_2', \ldots, \varepsilon_{l^*}^{(l^*-1)}$). From (35.6) it follows that

$$\left\{\frac{\kappa\kappa'\kappa''\cdots}{\mathfrak{r}}\right\} = \left\{\frac{q}{\mathfrak{r}}\right\} = \zeta^*,$$

and hence, if ρ is a primary number for $\mathfrak{r}$, we deduce from Theorem 140 (p. 202) that we also have

$$\left\{\frac{\rho}{q}\right\} = \left\{\frac{\rho}{\mathfrak{q}}\right\}\left\{\frac{\rho}{\mathfrak{q}'}\right\}\left\{\frac{\rho}{\mathfrak{q}''}\right\}\cdots = \zeta^*. \tag{35.9}$$

On the other hand, it follows from (35.6) by Lemma 44 that

$$\left\{\frac{\rho}{\mathfrak{q}'}\right\} = 1, \left\{\frac{\rho}{\mathfrak{q}''}\right\} = 1, \ldots;$$

hence it follows from (35.9) that $\left\{\frac{\rho}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\} = \zeta^*$ and hence that

$$\left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\} \neq 1. \tag{35.10}$$

Similarly we deduce from (35.7) the relation

$$\left\{\frac{\mathfrak{q}_1}{\mathfrak{r}}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{q}_1}\right\} \neq 1. \tag{35.11}$$

Now we determine a power ρ^e of ρ such that $\left\{\frac{\kappa\rho^e}{\mathfrak{q}_1}\right\} = 1$ and consider the Kummer field $k(\sqrt[l]{\kappa\rho^e}, \zeta)$, Since $\mathfrak{q}$ (by hypothesis) and $\mathfrak{r}$ (by (35.8)) are prime ideals of the second kind it follows by means of Lemma 43 that the relative discriminant of this field has only the two prime ideal factors $\mathfrak{q}$ and $\mathfrak{r}$. By Lemma 35 (p. 288) we deduce that $k(\sqrt[l]{\kappa\rho^e}, \zeta)$ has at most l genera. The prime ideal $\mathfrak{r}$ is the l-th power of a prime ideal $\mathfrak{R}$ in $k(\sqrt[l]{\kappa\rho^e}, \zeta)$. The two characters of $\mathfrak{R}$ in this field are

$$\left\{\frac{\rho, \kappa\rho^e}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\} \quad \text{and} \quad \left\{\frac{\rho, \kappa\rho^e}{\mathfrak{r}}\right\} = \left\{\frac{\kappa}{\mathfrak{r}}\right\}^{-1} = \left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\}^{-1}$$

and from these we obtain the characters of $\mathfrak{R}^2, \mathfrak{R}^3, \ldots, \mathfrak{R}^l$. According to (35.10) the l ideals $\mathfrak{R}, \mathfrak{R}^2, \ldots, \mathfrak{R}^l$ determine l distinct genera and by the same formula (35.10) the product of the two characters of each of these ideals is 1. It follows that this holds for every ideal in $k(\sqrt[l]{\kappa\rho^e}, \zeta)$. Since $\left\{\frac{\kappa\rho^e}{\mathfrak{q}_1}\right\} = 1$ the prime ideal $\mathfrak{q}_1$ splits in $k(\sqrt[l]{\kappa\rho^e}, \zeta)$; the characters of a prime factor of $\mathfrak{q}_1$ are

$$\left\{\frac{\kappa_1, \kappa\rho^e}{\mathfrak{q}}\right\} = \left\{\frac{\kappa_1}{\mathfrak{q}}\right\} \quad \text{and} \quad \left\{\frac{\kappa_1, \kappa\rho^e}{\mathfrak{r}}\right\} = \left\{\frac{\kappa_1}{\mathfrak{r}}\right\}^e$$

and so we have $\left\{\frac{\kappa_1}{\mathfrak{q}}\right\}\left\{\frac{\kappa_1}{\mathfrak{r}}\right\}^e = 1$. Since, on the other hand, we have

$$\left\{\frac{\kappa\rho^e}{\mathfrak{q}_1}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{q}_1}\right\}\left\{\frac{\mathfrak{r}}{\mathfrak{q}_1}\right\}^e = 1$$

it follows by means of (35.11) that $\left\{\frac{\mathfrak{q}_1}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{q}_1}\right\}$.

Lemma 46. *Let $\mathfrak{p}$ be a prime ideal of the first kind and $\mathfrak{q}$ a prime ideal of the second kind in $k(\zeta)$. If $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} = 1$ then $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\} = 1$ also.*

Proof. Let π and κ be primary numbers for $\mathfrak{p}$ and $\mathfrak{q}$ respectively. Suppose that $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} = 1$ but $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\} \neq 1$. By Theorem 152 (p. 254) there would be a prime ideal $\mathfrak{r}$ distinct from $\mathfrak{p}$ and $\mathfrak{q}$ such that

$$\left\{\frac{\pi}{\mathfrak{r}}\right\} \neq 1, \ \left\{\frac{\kappa}{\mathfrak{r}}\right\} \neq 1, \tag{35.12}$$

$$\left\{\frac{\zeta}{\mathfrak{r}}\right\} = 1, \ \left\{\frac{\varepsilon_1}{\mathfrak{r}}\right\} = 1, \ldots, \ \left\{\frac{\varepsilon_{l^*}}{\mathfrak{r}}\right\} = 1, \tag{35.13}$$

where $\varepsilon_1, \ldots, \varepsilon_{l^*}$ are the units determined in Sect. 166 (denoted there by ε_1, $\varepsilon_2', \ldots, \varepsilon_{l^*}^{(l^*-1)}$). According to (35.13) $\mathfrak{r}$ is a prime ideal of the second kind. If ρ is a primary number for $\mathfrak{r}$ we have $\left\{\frac{\rho}{\mathfrak{p}}\right\} \neq 1$; for if $\left\{\frac{\rho}{\mathfrak{p}}\right\} = 1$ it would follow from Lemma 44 (p. 318) that $\left\{\frac{\pi}{\mathfrak{r}}\right\} = 1$, which contradicts the first equation in (35.12). Thus we can find a power ρ^e of ρ such that $\left\{\frac{\kappa\rho^e}{\mathfrak{p}}\right\} = 1$.

Since $\mathfrak{r}$ and $\mathfrak{q}$ are prime ideals of the second kind it follows by means of Lemma 43 (p. 315) and Theorem 148 (p. 227) that the relative discriminant of the field $k(\sqrt[l]{\kappa\rho^e}, \zeta)$ has only the two prime ideal factors $\mathfrak{q}$ and $\mathfrak{r}$. Now, by (35.12), we have $\left\{\frac{\kappa}{\mathfrak{r}}\right\} \neq 1$ and by Lemma 45 (p. 318)

$$\left\{\frac{\kappa}{\mathfrak{r}}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\};$$

hence it follows, as in the proof of Lemma 45, that for every ideal in $k(\sqrt[l]{\kappa\rho^e}, \zeta)$ the product of its two characters must be equal to 1. Since $\left\{\frac{\kappa\rho^e}{\mathfrak{p}}\right\} = 1$ the prime ideal $\mathfrak{p}$ splits in $k(\sqrt[l]{\kappa\rho^e}, \zeta)$; each prime factor of $\mathfrak{p}$ has the two characters

$$\left\{\frac{\pi, \kappa\rho^e}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} \quad \text{and} \quad \left\{\frac{\pi, \kappa\rho^e}{\mathfrak{r}}\right\} = \left\{\frac{\pi}{\mathfrak{r}}\right\}^e.$$

Since, by hypothesis, the first character is equal to 1 it follows from what we have just proved that $\left\{\frac{\pi}{\mathfrak{r}}\right\} = 1$ which contradicts (35.12). Hence our hypothesis that $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\} \neq 1$ leads to a contradiction and so $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\} = 1$ as asserted in the lemma.

Lemma 47. *If* $\mathfrak{q}$ *is a prime ideal of the second kind and* $\mathfrak{p}$ *is a prime ideal of the first kind then* $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\} = \left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}$.

Proof. We proceed precisely as in the proof of Lemma 45, replacing the prime ideal $\mathfrak{q}_1$ by $\mathfrak{p}$ and then in the course of the proof in order to derive the relation corresponding to (35.11) we use Lemma 46 instead of Lemma 44.

§169. A Lemma About the Product $\prod'_{(\mathfrak{w})}\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\}$ Where $\mathfrak{w}$ Runs Over All Prime Ideals Distinct from $\mathfrak{l}$

We are now in a position to derive the following lemma.

Lemma 48. *If* ν *and* μ *are integers prime to* $\mathfrak{l}$ *and* μ *is congruent modulo* $\mathfrak{l}^l$ *to the* l*-th power of an integer in* $k(\zeta)$ *then*

$$\prod_{(\mathfrak{w})}{}'\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\} = 1,$$

where the product is taken over all prime ideals $\mathfrak{w}$ *distinct from* $\mathfrak{l}$.

Proof. Under the hypothesis made about μ we can obviously write μ as a product of primary numbers for prime ideals divided by the l-th power of an integer in $k(\zeta)$. If in particular ν is equal to a primary number for a prime ideal $\mathfrak{q}$ of the second kind then the assertion of the lemma follows at once from Lemmas 45 and 47, i.e., under the conditions imposed on μ we have

$$\prod_{(\mathfrak{w})}{}'\left\{\frac{\kappa,\mu}{\mathfrak{w}}\right\} = 1. \tag{35.14}$$

Now we consider the Kummer field $k(\sqrt[l]{\mu},\zeta)$. If r is the number of characters which determine the genus of an ideal class of this field then, according to Lemma 35 (p. 288), there are at most l^{r-1} genera in this field. Let $\gamma_1, \ldots, \gamma_r$ be any r l-th roots of unity whose product is 1. Then we can establish, precisely as in the proof of Theorem 164 (p. 306), that there are ideals in the field $k(\sqrt[l]{\mu},\zeta)$ whose characters coincide with $\gamma_1, \ldots, \gamma_r$. To do this we have only to add to the conditions (34.6) and (34.7) the further conditions on the prime ideal $\mathfrak{p}$ occurring there:

$$\left\{\frac{\zeta}{\mathfrak{p}}\right\} = 1, \left\{\frac{\varepsilon_1}{\mathfrak{p}}\right\} = 1, \ldots, \left\{\frac{\varepsilon_{l^*}}{\mathfrak{p}}\right\} = 1,$$

where $\varepsilon_1, \ldots, \varepsilon_{l^*}$ are the units introduced in Sect. 166 (denoted there by ε_1, $\varepsilon_2', \ldots, \varepsilon_{l^*}^{(l^*-1)}$). In this way of course we obtain the result that $\mathfrak{p}$ is actually a

prime ideal of the second kind. Hence we may refer to Lemmas 45 and 47 and apply the reciprocity law in the same way as we did in Theorem 164. Instead of Theorem 163 which was used there we bring into play here the formula (35.14). At the same time it follows that there are actually l^{r-1} genera in $k(\sqrt[l]{\mu}, \zeta)$ and hence that for each of them the product of the r characters must always be 1. We now apply these facts to prove Lemma 48 for the case where ν is a unit and then for the case in which ν is a primary number for a prime ideal of the first kind.

Again let $\varepsilon_1, \dots, \varepsilon_{l^*}$ be the l^* units mentioned above; let $\mathfrak{l}_1, \dots, \mathfrak{l}_t$ be, as in Sect. 149, the t distinct prime ideals which divide the relative discriminant of $k(\sqrt[l]{\mu}, \zeta)$; let prime ideals $\mathfrak{l}_t, \mathfrak{l}_{t-1}, \dots, \mathfrak{l}_{r+1}$ be chosen from among them as in Sect. 149; let $\lambda_{r+1}, \dots, \lambda_t$ be primary numbers for $\mathfrak{l}_{r+1}, \dots, \mathfrak{l}_t$ respectively; finally, let ξ be any unit of $k(\zeta)$. By Theorem 152 (p. 254) there is a prime ideal $\mathfrak{q}$ such that

$$\left\{\frac{\xi}{\mathfrak{q}}\right\} = 1,\ \left\{\frac{\varepsilon_1}{\mathfrak{q}}\right\} = 1, \dots,\ \left\{\frac{\varepsilon_{l^*}}{\mathfrak{q}}\right\} = 1,\ \left\{\frac{\mu}{\mathfrak{q}}\right\} = 1, \tag{35.15}$$

$$\left\{\frac{\lambda_{r+1}}{\mathfrak{q}}\right\} = \left\{\frac{\xi}{\mathfrak{l}_{r+1}}\right\}^m,\ \left\{\frac{\lambda_{r+2}}{\mathfrak{q}}\right\} = \left\{\frac{\xi}{\mathfrak{l}_{r+2}}\right\}^m, \dots,\ \left\{\frac{\lambda_t}{\mathfrak{q}}\right\} = \left\{\frac{\xi}{\mathfrak{l}_t}\right\}^m, \tag{35.16}$$

where m is a certain exponent prime to l. Let κ be a primary number of $\mathfrak{q}$. According to the equation $\left\{\frac{\mu}{\mathfrak{q}}\right\} = 1$ the prime ideal $\mathfrak{q}$ splits in $k(\sqrt[l]{\mu}, \zeta)$ and according to the remaining equations (35.15) $\mathfrak{q}$ is a prime ideal of the first kind. Since we have (as we see from (35.16) and Lemmas 45 and 47)

$$\left\{\frac{\xi^{-m}\kappa, \mu}{\mathfrak{l}_{r+1}}\right\} = 1, \dots,\ \left\{\frac{\xi^{-m}\kappa, \mu}{\mathfrak{l}_t}\right\} = 1, \tag{35.17}$$

the r characters of each prime factor of $\mathfrak{q}$ have the values

$$\left\{\frac{\xi^{-m}\kappa, \mu}{\mathfrak{l}_1}\right\},\ \left\{\frac{\xi^{-m}\kappa, \mu}{\mathfrak{l}_2}\right\}, \dots,\ \left\{\frac{\xi^{-m}\kappa, \mu}{\mathfrak{l}_r}\right\}.$$

Now according to what was proved above the product of these characters must be 1; referring to (35.17) and the last equation in (35.15) we deduce the relation

$$\prod_{(\mathfrak{w})}{}' \left\{\frac{\xi^{-m}\kappa, \mu}{\mathfrak{w}}\right\} = 1$$

where the product is taken over all prime ideals $\mathfrak{w}$ distinct from $\mathfrak{l}$. Hence it follows with the help of (35.14) that

$$\prod_{(\mathfrak{w})}{}' \left\{\frac{\xi^{-m}, \mu}{\mathfrak{w}}\right\} = 1 \quad \text{and so} \quad \prod_{(\mathfrak{w})}{}' \left\{\frac{\xi, \mu}{\mathfrak{w}}\right\} = 1. \tag{35.18}$$

Thus Lemma 48 holds also in the case where ν is any unit in $k(\zeta)$.

Now let $\mathfrak{p}$ be any prime ideal of the first kind which satisfies the condition that $\left\{\frac{\mu}{\mathfrak{p}}\right\} = 1$ and hence splits in $k(\sqrt[l]{\mu}, \zeta)$. The r characters of each prime ideal factor of $\mathfrak{p}$ are

$$\left\{\frac{\xi\pi,\mu}{\mathfrak{l}_1}\right\}, \left\{\frac{\xi\pi,\mu}{\mathfrak{l}_2}\right\}, \ldots, \left\{\frac{\xi\pi,\mu}{\mathfrak{l}_r}\right\},$$

where π is a primary number for $\mathfrak{p}$ and ξ is a suitable unit of $k(\zeta)$. Since the product of these characters is 1 we have, as before,

$$\prod_{(\mathfrak{w})}'\left\{\frac{\xi\pi,\mu}{\mathfrak{w}}\right\} = 1$$

and hence, by (35.18),

$$\prod_{(\mathfrak{w})}'\left\{\frac{\pi,\mu}{\mathfrak{w}}\right\} = 1.$$

If, finally, $\mathfrak{p}$ is a prime ideal of the first kind prime to μ such that $\left\{\frac{\mu}{\mathfrak{p}}\right\} \neq 1$ then we determine a prime ideal $\mathfrak{q}$ of the second kind such that $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} \neq 1$; by Lemma 44 we also have $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\} \neq 1$. If κ is a primary number for $\mathfrak{q}$ and κ^e is a power of κ such that $\left\{\frac{\mu\kappa^e}{\mathfrak{p}}\right\} = 1$ then, by what we have just proved,

$$\prod_{(\mathfrak{w})}'\left\{\frac{\pi,\mu\kappa^e}{\mathfrak{w}}\right\} = 1$$

and since, by Lemma 47, we also have

$$\prod_{(\mathfrak{w})}'\left\{\frac{\pi,\kappa}{\mathfrak{w}}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\}^{-1}\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} = 1,$$

it follows that we have

$$\prod_{(\mathfrak{w})}'\left\{\frac{\pi,\mu}{\mathfrak{w}}\right\} = 1. \tag{35.19}$$

So Lemma 48 holds if ν is a primary number for a prime ideal of the first kind. From (35.14), (35.18) and (35.19) we see that Lemma 48 holds in general.

§170. The Symbol $\{\nu, \mu\}$ and the Reciprocity Law Between Any Two Prime Ideals

We have now reached in a surprisingly simple way the new foundation of the theory of regular Kummer fields on which we set our sights at the beginning of this chapter. If ν and μ are any two integers of $k(\zeta)$ we set

$$\{\nu,\mu\} = \Big(\prod_{(\mathfrak{w})}{}' \Big\{\frac{\nu,\mu}{\mathfrak{w}}\Big\}\Big)^{-1} \tag{35.20}$$

where again the product $\prod_{(\mathfrak{w})}{}'$ is taken over all prime ideals $\mathfrak{w}$ distinct from $\mathfrak{l}$. The *symbol* $\{\nu,\mu\}$ is an l-th root of unity which is completely determined by the numbers ν and μ and from (29.9) (p. 240) we deduce the formulae

$$\left.\begin{aligned} \{\nu_1\nu_2,\mu\} &= \{\nu_1,\mu\}\{\nu_2,\mu\} \\ \{\nu,\mu_1\mu_2\} &= \{\nu,\mu_1\}\{\nu,\mu_2\} \\ \{\nu,\mu\}\{\mu,\nu\} &= 1, \end{aligned}\right\} \tag{35.21}$$

where ν, ν_1, ν_2, μ, μ_1, μ_2 are integers in $k(\zeta)$. Let r be a primitive root modulo l and $s = (\zeta : \zeta^r)$ the corresponding automorphism in the group of $k(\zeta)$. Then

$$\{s\nu, s\mu\} = \{\nu,\mu\}^r. \tag{35.22}$$

We have also the following result.

Lemma 49. *If ν and μ are any two primary numbers of the field $k(\zeta)$ then the symbol $\{\nu,\mu\}$ has the value* 1.

Proof. If a is any rational integer prime to ν and l then it follows from Theorem 140 (p. 202) that we have

$$\{\nu,a\} = \Big\{\frac{\nu}{a}\Big\}^{-1}\Big\{\frac{a}{\nu}\Big\} = 1. \tag{35.23}$$

Since we have taken μ to be a primary number the product $\mu \cdot s^{\frac{1}{2}(l-1)}\mu$ is congruent modulo $\mathfrak{l}^{l-1}$ to a rational integer. Consequently we can also determine a rational integer a modulo $\mathfrak{l}^l$ in such a way that

$$a\cdot\mu\cdot s^{\frac{1}{2}(l-1)}\mu \equiv 1 \pmod{\mathfrak{l}^l}$$

and moreover we can choose a prime to ν. Applying Lemma 48 we have

$$\{\nu,a\}\{\nu,\mu\}\{\nu,s^{\frac{1}{2}(l-1)}\mu\} = \{\nu,a\cdot\mu\cdot s^{\frac{1}{2}(l-1)}\mu\} = 1;$$

hence, by (35.23), we also have

$$\{\nu,\mu\}\{\nu, s^{\frac{1}{2}(l-1)}\mu\} = 1.$$

Similarly we prove that

$$\{\nu, s^{\frac{1}{2}(l-1)}\mu\}\{s^{\frac{1}{2}(l-1)}\nu, s^{\frac{1}{2}(l-1)}\mu\} = 1.$$

From formula (35.22) we have

$$\{\nu,\mu\}\{s^{\frac{1}{2}(l-1)}\nu, s^{\frac{1}{2}(l-1)}\mu\} = 1.$$

The last three equations taken together lead to the result that

$$\{\nu,\mu\}^2 = 1.$$

Hence $\{\nu,\mu\} = 1$ and the proof of Lemma 49 is complete.

If we choose ν and μ in particular to be primary numbers for arbitrary prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ in $k(\zeta)$ then the assertion of Lemma 49 is equivalent to the general reciprocity law (Theorem 161 (p. 289)) for these prime ideals $\mathfrak{p}$ and $\mathfrak{q}$.

§171. Coincidence of the Symbols $\{\nu,\mu\}$ and $\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}$

We deduce from Theorem 151 (applying it only in the case where $\mathfrak{w} \neq \mathfrak{l}$) that $\{\nu,\mu\}$ always has the value 1 if ν is the relative norm of an integer in the field $k(\sqrt[l]{\mu},\zeta)$; we now go on to prove that $\{\alpha,\mu\}$ also has the value 1 provided that the integer α is a norm residue of the field $k(\sqrt[l]{\mu},\zeta)$ modulo $\mathfrak{l}$. To see this, let us suppose for the sake of brevity that both numbers α and μ are prime to $\mathfrak{l}$; let $\alpha \equiv N_k(\mathsf{A}) \pmod{\mathfrak{l}^l}$, where $N_k(\mathsf{A})$ is the relative norm of an integer A in $k(\sqrt[l]{\mu},\zeta)$; then $\alpha \cdot (N_k(\mathsf{A}))^{l-1}$ is obviously congruent modulo $\mathfrak{l}^l$ to the l-th power of an integer. Hence, using formula (35.21) and referring to our earlier remarks and Lemma 48, we have

$$\{\alpha\cdot(N_k(\mathsf{A}))^{l-1},\mu\} = \{\alpha,\mu\}\{N_k(\mathsf{A}),\mu\}^{l-1} = \{\alpha,\mu\} = 1$$

as asserted. If one of the numbers α, μ is divisible by $\mathfrak{l}$ or both are, then the proof of this result can be carried out without difficulty using the same kind of argument.

If μ is an integer of $k(\zeta)$ prime to $\mathfrak{l}$ then we can easily deduce from (35.20) that

$$\{\zeta,\mu\} = \zeta^{(1-n(\mu))/l};$$

accordingly the symbol $\{\nu,\mu\}$ satisfies the same conditions as those we established at the end of Sect. 133 for the symbol $\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}$; and so, if we use the definition of the symbol $\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}$ given on p. 251, it follows that

$$\{\nu,\mu\} = \left\{\frac{\nu,\mu}{\mathfrak{l}}\right\};$$

In this equation we recognise Theorem 163 (p. 305).

If, in particular, both numbers ν and μ are prime to $\mathfrak{l}$ and $\bar{\nu}$ and $\bar{\mu}$ are integers of $k(\zeta)$ congruent to ν and μ respectively modulo $\mathfrak{l}^l$ then, by using Lemma 48, we deduce easily that

$$\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\} = \left\{\frac{\bar{\nu},\bar{\mu}}{\mathfrak{l}}\right\}.$$

From this, in view of the formula (35.21), we deduce the following result: if the numbers ν and μ are both prime to $\mathfrak{l}$ and

$$\begin{aligned} \nu &\equiv a^l(1+\lambda)^{n_1}(1+\lambda^2)^{n_2}\cdots(1+\lambda^{l-1})^{n_{l-1}} \pmod{\mathfrak{l}^l}, \\ \mu &\equiv b^l(1+\lambda)^{m_1}(1+\lambda^2)^{m_2}\cdots(1+\lambda^{l-1})^{m_{l-1}} \pmod{\mathfrak{l}^l}, \end{aligned}$$

where a and b and the exponents $n_1, n_2, \dots, n_{l-1}, m_1, m_2, \dots, m_{l-1}$ are rational integers, then there is an equation of the form

$$\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\} = \zeta^{L(n_1,\dots,n_{l-1};m_1,\dots,m_{l-1})}$$

where L is a homogeneous bilinear function of both sets of variables $n_1, \dots, n_{l-1}$; $m_1, \dots, m_{l-1}$ and the coefficients of L are rational integers which depend only on l and which, for a given prime l, can be easily calculated by making special choices of the numbers ν and μ.

Now that the symbol $\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}$ has been defined and its most important properties derived we may relax the restriction hitherto in force in this chapter to Kummer fields with relative discriminant prime to l; then, precisely as above, we obtain proofs of Theorems 164 (p. 306), 165 (p. 308), 166 (p. 309) and especially the fundamental Theorem 167 (p. 309). With the help of Theorem 167 and appropriate use of Theorem 152 (p. 254) it can also be shown that if ν and μ are any two integers of $k(\zeta)$ such that $\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\} = 1$ and μ is not the l-th power of an integer in $k(\zeta)$ then the number ν must be a norm residue of the Kummer field $k(\sqrt[l]{\mu},\zeta)$ modulo $\mathfrak{l}$. Thus Theorem 151 (p. 248) holds also for the case $\mathfrak{w} = \mathfrak{l}$ and from this we deduce that Theorem 150 (p. 233) is also valid for $\mathfrak{w} = \mathfrak{l}$. Thus, in the method of developing the theory of Kummer fields which we have been describing, Theorems 150 and 151 for $\mathfrak{w} = \mathfrak{l}$ appear (in contrast to the earlier development) as the keystone of the whole construction.

36. The Diophantine Equation $\alpha^m + \beta^m + \gamma^m = 0$

§172. The Impossibility of the Diophantine Equation $\alpha^l + \beta^l + \gamma^l = 0$ for a Regular Prime Number Exponent l

Fermat advanced the conjecture that the equation

$$a^m + b^m + c^m = 0$$

is not solvable in nonzero rational integers a, b, c if $m > 2$. Although there were already remarkable isolated results about this Fermat equation before the time of Kummer (*Abel* (1), *Cauchy* (1, 2). *Dirichlet* (1, 2, 3), *Lamé* (1, 2, 3), *Lebesgue* (1, 2, 3)) nevertheless Kummer, using the theory of ideals in regular cyclotomic fields, was the first to succeed in completely proving Fermat's conjecture for a very extensive class of exponents m. The most important result obtained by Kummer is as follows.

Theorem 168. *If l is a regular prime number and α, β, γ are any integers of the cyclotomic field of the l-th roots of unity, all of them nonzero, then the equation*

$$\alpha^l + \beta^l + \gamma^l = 0 \tag{36.1}$$

never holds (*Kummer* (1, 9, 11)).

Proof. Let $\zeta = e^{2\pi i/l}$, $\lambda = 1 - \zeta$, $\mathfrak{l} = (\lambda)$. We suppose, in contradiction to the assertion of the theorem, that the equation (36.1) does have a solution in integers α, β, γ of the field $k(\zeta)$. We distinguish two cases: (1) in which none of the three integers α, β, γ is divisible by $\mathfrak{l}$, (2) in which at least one of them is divisible by $\mathfrak{l}$.

(1) In the first case the values 3 and 5 for the exponent l are certainly excluded. To see this in the case where $l = 3$ suppose each of the three integers $\alpha, \beta, \gamma \equiv \pm 1 \pmod{\mathfrak{l}}$ and consequently each of the three powers $\alpha^3, \beta^3, \gamma^3 \equiv \pm 1 \pmod{\mathfrak{l}^3}$; from this it follows that the sum of these three powers would turn out to be congruent to ± 1 or ± 3 modulo $\mathfrak{l}^3$, which is not consistent with equation (36.1). We reach a similar contradiction with $l = 5$ if we notice that in this case each of the three integers $\alpha, \beta, \gamma \equiv \pm 1$ or $\pm 2 \pmod{\mathfrak{l}}$ and so each of the powers $\alpha^5, \beta^5, \gamma^5 \equiv \pm 1$ or $\pm 32 \pmod{\mathfrak{l}^5}$.

So we consider the equation (36.1) where $l \geq 7$. If the equation holds for the three integers α, β, γ then obviously we also have $(\alpha^*)^l + (\beta^*)^l + (\gamma^*)^l = 0$ if α^*, β^*, γ^* are products of α, β, γ respectively by arbitrary l-th roots of unity. In consequence of this we may assume from now on that the three numbers α, β, γ satisfying (36.1) are semiprimary. We now write (36.1) in the form

$$(\alpha+\beta)(\alpha+\zeta\beta)(\alpha+\zeta^2\beta)\cdots(\alpha+\zeta^{l-1}\beta) = -\gamma^l. \tag{36.2}$$

If two of the factors on the left hand side, say $\alpha+\zeta^u\beta$ and $\alpha+\zeta^{u+g}\beta$, have a common factor this must also divide $(\zeta^g-1)\alpha$ and $(1-\zeta^g)\beta$; since $\dfrac{1-\zeta^g}{1-\zeta}$ is a unit and $\mathfrak{l}$ does not divide γ, this common factor must be a common factor of α and β. Since each prime factor which divides only *one* of the factors on the left hand side of (36.2) must obviously (on account of this equation) occur to a power with exponent divisible by l, it follows that the l factors on the left hand side of (36.2) can be decomposed as follows:

$$\begin{aligned} \alpha+\beta &= \mathfrak{i}^l\mathfrak{a}, \\ \alpha+\zeta\beta &= \mathfrak{i}_1^l\mathfrak{a}, \\ \alpha+\zeta^2\beta &= \mathfrak{i}_2^l\mathfrak{a}, \\ &\cdots \\ \alpha+\zeta^{l-1}\beta &= \mathfrak{i}_{l-1}^l\mathfrak{a}, \end{aligned}$$

where $\mathfrak{a}$ is the greatest common (ideal) divisor of the numbers α and β and $\mathfrak{i}$, $\mathfrak{i}_1$, $\mathfrak{i}_2$, ..., $\mathfrak{i}_{l-1}$ are ideals in $k(\zeta)$. Since in particular $\alpha+\zeta^{l-1}\beta$ is prime to $\mathfrak{l}$ we can find an l-th root of unity ζ^* such that $\zeta^*(\alpha+\zeta^{l-1}\beta)$ is semiprimary. We set

$$\mu = \frac{\alpha}{\zeta^*(\alpha+\zeta^{l-1}\beta)}, \quad \rho = \frac{\beta}{\zeta^*(\alpha+\zeta^{l-1}\beta)}.$$

Then we have

$$\left.\begin{aligned} \mu+\rho &= \left(\frac{\mathfrak{i}}{\mathfrak{i}_{l-1}}\right)^l \\ \mu+\zeta\rho &= \left(\frac{\mathfrak{i}_1}{\mathfrak{i}_{l-1}}\right)^l \\ &\cdots \\ \mu+\zeta^{l-2}\rho &= \left(\frac{\mathfrak{i}_{l-2}}{\mathfrak{i}_{l-1}}\right)^l \end{aligned}\right\} \tag{36.3}$$

i.e. we have

$$\left(\frac{\mathfrak{i}}{\mathfrak{i}_{l-1}}\right)^l \sim 1, \left(\frac{\mathfrak{i}_1}{\mathfrak{i}_{l-1}}\right)^l \sim 1, \ldots, \left(\frac{\mathfrak{i}_{l-2}}{\mathfrak{i}_{l-1}}\right)^l \sim 1$$

and in addition

$$\mu+\zeta^{l-1}\rho = (\zeta^*)^{-1}. \tag{36.4}$$

If h is the number of ideal classes in $k(\zeta)$ then we have on the other hand

$$\left(\frac{\mathfrak{i}}{\mathfrak{i}_{l-1}}\right)^h \sim 1, \left(\frac{\mathfrak{i}_1}{\mathfrak{i}_{l-1}}\right)^h \sim 1, \ldots, \left(\frac{\mathfrak{i}_{l-2}}{\mathfrak{i}_{l-1}}\right)^h \sim 1$$

and since h is prime to l it follows that

$$\frac{\mathfrak{i}}{\mathfrak{i}_{l-1}} \sim 1,\ \frac{\mathfrak{i}_1}{\mathfrak{i}_{l-1}} \sim 1, \ldots,\ \frac{\mathfrak{i}_{l-2}}{\mathfrak{i}_{l-1}} \sim 1.$$

From this we see, referring to Theorem 127 (p. 173), that the equations (36.3) can be put in the form

$$\mu + \zeta^u \rho = \zeta^{e_u} \varepsilon_u \alpha_u^l \quad (u = 0, 1, 2, \ldots, l-2), \tag{36.5}$$

where the e_u are certain rational integer exponents, the ε_u suitable *real* units of the cyclotomic field $k(\zeta)$ and the α_u are integers or fractions in $k(\zeta)$ with numerators and denominators prime to $\mathfrak{l}$. Since the l-th power of each number α_u is congruent modulo $\mathfrak{l}^l$ to a certain rational number a_u we deduce from (36.5) the congruences

$$\mu + \zeta^u \rho \equiv \zeta^{e_u} \varepsilon_u a_u \pmod{\mathfrak{l}^l} \quad (u = 0, 1, 2, \ldots, l-2). \tag{36.6}$$

To these congruences we apply the automorphism $(\zeta : \zeta^{-1})$; denoting the images of μ and ρ under this automorphism by μ' and ρ' respectively we have

$$\mu' + \zeta^{-u} \rho' \equiv \zeta^{-e_u} \varepsilon_u a_u \pmod{\mathfrak{l}^l} \quad (u = 0, 1, 2, \ldots, l-2). \tag{36.7}$$

From (36.6) and (36.7) we obtain

$$\mu + \zeta^u \rho \equiv \zeta^{2e_u} \mu' + \zeta^{2e_u - u} \rho' \pmod{\mathfrak{l}^l} \quad (u = 0, 1, 2, \ldots, l-2). \tag{36.8}$$

Setting $\mu \equiv m$ and $\rho \equiv r \pmod{\mathfrak{l}^2}$ where m and r are rational integers we deduce from (36.8) that

$$m + \zeta^u r \equiv \zeta^{2e_u} m + \zeta^{2e_u - u} r \pmod{\mathfrak{l}^2} \tag{36.9}$$

and, from the general relation $\zeta^g \equiv 1 - g\lambda \pmod{\mathfrak{l}^2}$, (36.9) yields the congruence

$$2e_u(m + r) \equiv 2ru \pmod{l}.$$

On the other hand we deduce from (36.4) that $m + r \equiv 1 \pmod{l}$ and hence we have

$$e_u \equiv ru \pmod{l} \quad (u = 0, 1, 2, \ldots, l-2).$$

If we take the congruences (36.8) for $u = 0, 1, 2, 3$ and use the relations we have just established then, by eliminating the numbers μ, ρ, μ', ρ', we obtain

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & \zeta & \zeta^{2r} & \zeta^{2r-1} \\ 1 & \zeta^2 & (\zeta^{2r})^2 & (\zeta^{2r-1})^2 \\ 1 & \zeta^3 & (\zeta^{2r})^3 & (\zeta^{2r-1})^3 \end{vmatrix} \equiv 0 \pmod{\mathfrak{l}^l},$$

i.e.

$$(1-\zeta)(1-\zeta^{2r})(1-\zeta^{2r-1})(\zeta-\zeta^{2r})(\zeta-\zeta^{2r-1})(\zeta^{2r}-\zeta^{2r-1}) \equiv 0 \pmod{\mathfrak{l}^l}. \tag{36.10}$$

We claim that none of the factors on the left hand side is 0. For otherwise we would have to have $r \equiv 0$ or $r \equiv 1$ or $r \equiv \frac{1}{2}$ modulo l. If we had $r \equiv 0 \pmod{l}$ then β would be congruent to 0 modulo $\mathfrak{l}$; if we had $r \equiv 1 \pmod{l}$ it would follow that $\beta \equiv \alpha + \beta$ or $\alpha \equiv 0 \pmod{\mathfrak{l}}$; in both cases we have a contradiction to our current hypothesis about the numbers α, β, γ. If we had $r \equiv \frac{1}{2} \pmod{l}$ we would have $\rho \equiv \frac{1}{2} \pmod{\mathfrak{l}}$, i.e. $2\beta \equiv \alpha+\beta$ or $\alpha \equiv \beta \pmod{\mathfrak{l}}$. Since, however, α, β, γ appear symmetrically in the equation (36.1) the same argument would lead to the conclusion that $\alpha \equiv \gamma \pmod{\mathfrak{l}}$; then we would have $\alpha^l + \beta^l + \gamma^l \equiv 3\alpha \equiv 0 \pmod{\mathfrak{l}}$, hence $\alpha \equiv 0 \pmod{\mathfrak{l}}$, which contradicts our assumption about α, β, γ. Thus each factor on the left hand side of the congruence is divisible by $\mathfrak{l}$ but not by $\mathfrak{l}^2$. Hence, when we recall our assumption that $l \geq 7$, we see that the congruence (36.10) is impossible.

(2) We now suppose, secondly, that in the equation (36.1) one of the three numbers - say γ - is divisible by $\mathfrak{l}$; suppose further that $\mathfrak{l}$ divides γ to the m-th power precisely. Then, if we replace γ by $\lambda^m\delta$, where δ is an integer of $k(\zeta)$ prime to $\mathfrak{l}$, the equation (36.1) takes the form

$$\alpha^l + \beta^l = \varepsilon\lambda^{lm}\delta^l; \tag{36.11}$$

with $\varepsilon = -1$. We shall now show that in general no equation of the form (36.11) can hold if α, β, δ are integers prime to $\mathfrak{l}$ and ε is any unit of the cyclotomic field $k(\zeta)$. To this end we suppose again that the numbers α and β are semiprimary and bear in mind that α^l and β^l are congruent modulo $\mathfrak{l}^{l+1}$ to rational integers; hence, by (36.11), $\varepsilon\lambda^{lm}\delta^l$ is also congruent modulo $\mathfrak{l}^{l+1}$ to a rational integer. It follows that we must have $m > 1$. Furthermore we see, by an argument similar to that in the previous case and recalling that $\alpha + \beta$ is semiprimary, that we have the following equations:

$$\left.\begin{aligned} \alpha+\beta &= \lambda^{l(m-1)+1}\mathfrak{i}^l\mathfrak{a}, \\ \alpha+\zeta\beta &= \lambda\mathfrak{i}_1^l\mathfrak{a}, \\ &\dots \\ \alpha+\zeta^{l-1}\beta &= \lambda\mathfrak{i}_{l-1}^l\mathfrak{a}, \end{aligned}\right\} \tag{36.12}$$

where $\mathfrak{i}, \mathfrak{i}_1, \dots, \mathfrak{i}_{l-1}$ and $\mathfrak{a}$ are ideals of $k(\zeta)$ prime to $\mathfrak{l}$. If, in particular, $l = 3$, then the class number of the field $k(\zeta)$ is equal to 1 and so every ideal of $k(\zeta)$ is a principal ideal. In this case we set $\mathfrak{a} = (\kappa)$, where κ is an integer of $k(\zeta)$, and write

$$\mu = \frac{\alpha}{\kappa}, \quad \rho = \frac{\beta}{\kappa}.$$

The equations (36.12) are transformed into

$$\left.\begin{aligned} \mu+\rho &= \lambda^{3(m-1)+1}\mathfrak{i}^l, \\ \mu+\zeta\rho &= \lambda\mathfrak{i}_1^l, \\ \mu+\zeta^2\rho &= \lambda\mathfrak{i}_2^l. \end{aligned}\right\} \tag{36.13}$$

In the case where $l > 3$ we form the numbers

$$\mu = \frac{\alpha\lambda}{\alpha + \zeta^{l-1}\beta}, \quad \rho = \frac{\beta\lambda}{\alpha + \zeta^{l-1}\beta};$$

these can also be written as fractions with numerators and denominators prime to $\mathfrak{l}$. From the first three and the last of equations (36.12) we obtain the equations

$$\left.\begin{aligned} \mu + \rho &= \lambda^{l(m-1)+1}\Big(\frac{\mathfrak{i}}{\mathfrak{i}_{l-1}}\Big)^l, \\ \mu + \zeta\rho &= \lambda\Big(\frac{\mathfrak{i}_1}{\mathfrak{i}_{l-1}}\Big)^l, \\ \mu + \zeta^2\rho &= \lambda\Big(\frac{\mathfrak{i}_2}{\mathfrak{i}_{l-1}}\Big)^l. \end{aligned}\right\} \tag{36.14}$$

As in case (1) above we conclude from these equations that we have again

$$\frac{\mathfrak{i}}{\mathfrak{i}_{l-1}} \sim 1, \quad \frac{\mathfrak{i}_1}{\mathfrak{i}_{l-1}} \sim 1, \quad \frac{\mathfrak{i}_2}{\mathfrak{i}_{l-1}} \sim 1$$

and in consequence we can write the equations (36.14) in the form

$$\left.\begin{aligned} \mu + \rho &= \frac{\varepsilon^*\lambda^{l(m-1)+1}(\gamma^*)^l}{\nu}, \\ \mu + \zeta\rho &= \frac{\lambda(\alpha^*)^l}{\nu}, \\ \mu + \zeta^2\rho &= \frac{\varepsilon\lambda(\beta^*)^l}{\nu} \end{aligned}\right\} \tag{36.15}$$

where ν, α^*, β^*, γ^* are integers prime to $\mathfrak{l}$ and ε and ε^* are units in $k(\zeta)$. According to (36.13) we have a set of equations like (36.15) also when $l = 3$. By eliminating μ and ρ we obtain, both for $l = 3$ and $l > 3$, an equation of the form

$$(\alpha^*)^l + \eta(\beta^*)^l = \eta^*\lambda^{l(m-1)}(\gamma^*)^l \tag{36.16}$$

where $\eta = -\dfrac{1-\zeta}{1-\zeta^2}\varepsilon$ and $\eta^* = \dfrac{\zeta(1-\zeta)}{1-\zeta^2}\varepsilon^*$ are units in $k(\zeta)$. Since $(\alpha^*)^l$ and $(\beta^*)^l$ are congruent modulo $\mathfrak{l}^l$ to rational integers and, as we proved earlier, $m > 1$, it follows from this equation (36.16) that η must also be congruent modulo $\mathfrak{l}^l$ to a rational integer and hence, by Theorem 156 (p. 265), η is the l-th power of a unit in $k(\zeta)$. Now in equation (36.16) write $\beta^*\eta^{-1/l}$ in place of β^*; this gives an equation of the same form as (36.11) except that the exponent m is reduced by 1. Repeated application of this procedure to equation (36.16) leads eventually to an equation of the form (36.11) with $m = 1$ and hence to a contradiction.

This completes the proof of Theorem 168.

§173. Further Investigations on the Impossibility of the Diophantine Equation $\alpha^l + \beta^l + \gamma^l = 0$

Kummer has proved, in addition to the above results, that the equation $\alpha^l + \beta^l + \gamma^l = 0$ is not solvable in integers α, β, γ of the cyclotomic fields of the l-th roots of unity in the case where l is a prime number which divides the class number h of $k(e^{2\pi i/l})$ to the first but not to any higher power and, in addition, the units satisfy certain conditions (*Kummer* (16)). Referring to the remark on p. 264 we see that this shows in particular that the Fermat conjecture is established for all exponents m not exceeding 100. The problem of proving that the Fermat conjecture is true in general still awaits a solution.

It still remains to study the equation $\alpha^m + \beta^m + \gamma^m = 0$ for the case where the exponent m is a power of 2. It is of course well known that the equation $a^2 + b^2 = c^2$ has infinitely many solutions in rational integers. We have in addition the following result.

Theorem 169. *If α, β, γ are nonzero integers of the quadratic field generated by $i = \sqrt{-1}$, then the equation*

$$\alpha^4 + \beta^4 = \gamma^2 \tag{36.17}$$

never holds.

Proof. Let us suppose, to the contrary, that there exist three integers α, β, γ which satisfy this equation. Set $\lambda = 1 + i$ and $\mathfrak{l} = (\lambda)$. First we see easily that one of the numbers α, β must be divisible by λ. Suppose, to the contrary, that α and β are both prime to λ and recall that an integer of $k(i)$ which is prime to λ is congruent to 1 or i modulo $\mathfrak{l}^2$; its square is thus congruent to ± 1 modulo $\mathfrak{l}^4$ and its fourth power is congruent to 1 modulo $\mathfrak{l}^6$. So if α and β are both prime to λ we have $\alpha^4 + \beta^4 \equiv 2 \pmod{\mathfrak{l}^6}$. Hence γ must be divisible by $\mathfrak{l}$ but by no higher power of $\mathfrak{l}$. If accordingly we set $\gamma = \lambda + \lambda^2\gamma'$, where γ' is again an integer of $k(i)$, then we find $\gamma^2 \equiv 2i \pmod{\mathfrak{l}^4}$ and hence $\gamma^2 \not\equiv \alpha^4 + \beta^4 \pmod{\mathfrak{l}^4}$, which is a contradiction. The case in which both numbers α and β are divisible by $\mathfrak{l}$ can obviously be excluded at once since then γ would be divisible by $\mathfrak{l}^2$ and so the power λ^4 may be cancelled from both sides of the equation (36.17).

Thus there remains only the possibility that one of the numbers α, β – say α – is divisible by $\mathfrak{l}$ while β and γ are prime to $\mathfrak{l}$. Accordingly we set $\alpha = \lambda^m\alpha^*$ where α^* is a number prime to $\mathfrak{l}$ and turn our attention to the more general equation

$$\beta^4 - \gamma^2 = \varepsilon\lambda^{4m}(\alpha^*)^4 \tag{36.18}$$

where ε is any unit in $k(i)$. From this equation (36.18) we derive (replacing γ by $-\gamma$ if need be) two equations of the form

$$\left.\begin{aligned} \beta^2 + \gamma &= \eta\lambda^{4m-2}(\alpha')^4 \\ \beta^2 - \gamma &= \vartheta\lambda^2(\beta')^4 \end{aligned}\right\} \tag{36.19}$$

where η and ϑ are units and α' and β' are integers of $k(i)$ prime to $\mathfrak{l}$. Adding the equations (36.19) and dividing the result by $\vartheta\lambda^2$ we obtain an equation

$$(\beta')^4 - \vartheta'\beta^2 = \eta'\lambda^{4m-4}(\alpha')^4 \tag{36.20}$$

where ϑ' and η' are units of $k(i)$. This equation certainly cannot hold if $m = 1$ since the numbers β', ϑ', β, η' and α' are all congruent to 1 modulo $\mathfrak{l}$. Thus we must have $m > 1$. In this case, however, it follows from our equation (36.20) considered as a congruence modulo $\mathfrak{l}^2$ that $\vartheta' \equiv 1 \pmod{\mathfrak{l}^2}$ and hence $\vartheta' = \pm 1$. If now we set $\beta = \gamma'$ or $\beta = i\gamma'$ according as $\vartheta = +1$ or -1 then the equation (36.19) takes the form of (36.17) except that m is reduced by 1. Appropriate repetition of this procedure leads to a contradiction.

From the Fermat theorem for the case $l = 3$ we can immediately deduce that there is no cubic equation with rational coefficients whose discriminant is 1 other than

$$x^3 - x \pm \tfrac{1}{3} = 0$$

and those derived from them by transformations $x = x' + a$ where a is a rational number (*Kronecker* (8)).

According to Hurwitz the general Fermat statement is equivalent to the assertion that the expression $\sqrt[m]{1 - x^m}$, where x is a positive proper fraction and m is a rational integer exponent greater than 2, is always irrational.

References

(The numbers in square brackets after each reference give the pages on which the reference is cited.)

Abel, N. H. (1): Extraits de quelques lettres à Holmboe (Œuvres complètes **2**, 254–262). [327]

Arndt, F. (1): Bemerkungen über die Verwandlung der irrationalen Quadratwurzel in einen Kettenbruch. J. Reine Angew. Math. **31** (1846), 343-358. [119]

Bachmann, P. (1): Zur Theorie der komplexen Zahlen. J. Reine Angew. Math. **67** (1867), 200–204. [152, 222]

Bachmann, P. (2): Die Lehre von der Kreisteilung und ihre Beziehungen zur Zahlentheorie. Leipzig 1872. [171]

Bachmann, P. (3): Ergänzung einer Untersuchung von Dirichlet. Math. Ann. **16** (1880), 537–550. [152]

Berkenbusch, H. (1): Über die aus den 8-ten Wurzeln der Einheit entspringenden Zahlen. Inauguraldissertation. Marburg 1891. [197]

Cauchy, A.L. (1): Mémoire sur la théorie des nombres. C. R. Acad. Sci. Paris **10** (1840) (Œuvres de Cauchy S 1.V, Extr. no. 74, 52–64). [219, 327]

Cauchy, A.L. (2): Mémoire sur diverses propositions relatives à la théorie des nombres (3 notes). C. R. Acad. Sci. Paris **25** (1847), pp. 132; 177; 242. (Œuvres de Cauchy S 1.X, 354–368). [327]

Cayley, A. (1): Tables des formes quadratiques binaires pour les déterminants négatifs depuis $D = -1$ jusqu'à $D = -100$, pour les déterminants positifs non carrés depuis $D = 2$ jusqu'à $D = 99$ et pour les treize déterminants négatifs irréguliers qui se trouvent dans le premier millier. J. Reine Angew. Math. **60** (1862), 357–372 (Collected Mathematical Papers **5**, 141–156). [119]

Dedekind, R. (1): Vorlesungen über Zahlentheorie von P. G. Lejeune Dirichlet, 2. bis 4. Aufl. Braunschweig 1871-1894. Supplement **11** [3, 5, 7, 11, 20, 45, 54, 55, 56, 62, 64, 66, 74, 115, 118, 147, 155, 162, 210, 213] and Supplement **7**. [171]

Dedekind, R. (2): Sur la théorie des nombres entiers algébriques, Paris 1877, 1–121. Reprint of Bull. des sciences math. et astron. Sér. 1 t. XI (1876) and Sér. 2 t. I (1877) (Gesammelte mathematische Werke **3**, 262–296). [3]

Dedekind, R. (3): Über die Anzahl der Ideal-Klassen in den verschiedenen Ordnungen eines endlichen Körpers. Braunschweig, 1877, 1–55 (Gesammelte mathematische Werke **1**, 105–157). [68, 74, 75, 155]

Dedekind, R. (4): Über die Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen. Abh. K. Ges. Wiss. Göttingen **23** (1878), 1–23 (Gesammelte mathematische Werke **1**. 202–230). [32]

Dedekind, R. (5): Sur la théorie des nombres complexes idéaux. (Extrait d'une lettre adressée à M. Hermite.) C. R. Acad. Sci. Paris **90** (1880), 1205–1207 (Gesammelte mathematische Werke **1**, 233–235). [170]

Dedekind, R. (6): Über die Diskriminanten endlicher Körper. Abh. K. Ges. Wiss. Göttingen **29** (1882), 1-56 (Gesammelte mathematische Werke **1**, 351-396). [22, 25, 69, 74]

Dedekind, R. (7): Über einen arithmetischen Satz von Gauss. Mitt. dtsch. math. Ges. Prag **1892**, 1-11 (Gesammelte mathematische Werke **2**, 28-38) and Über die Begründung der Idealtheorie. Nachr. K. Ges. Wiss. Göttingen **1895**, 106-113 (Gesammelte mathematische Werke **2**, 50-58). [12]

Dedekind, R. (8): Zur Theorie der Ideale. Nachr. K. Ges. Wiss. Göttingen **1894**, 272-277 (Gesammelte mathematische Werke **2**, 43-48). [99]

Dedekind, R. (9): Über eine Erweiterung des Symbols $(\mathfrak{a}, \mathfrak{b})$ in der Theorie der Moduln. Nachr. K. Ges. Wiss. Göttingen **1895**, 183-188 (Gesammelte mathematische Werke **2**, 59-85). [74]

Lejeune Dirichlet, G. (1): Mémoire sur l'impossibilité de quelques équations indéterminées du cinquième degré. Werke **1**, 1-20 (1825). [327]

Lejeune Dirichlet, G. (2): Mémoire sur l'impossibilité de quelques équations indéterminées du cinquième degré. J. Reine Angew. Math. **3** (1828), 354-375 (Werke **1**, 21-46). [327]

Lejeune Dirichlet, G. (3): Démonstration du théorème de Fermat pour le cas des 14ièmes puissances. J. Reine Angew. Math. **9** (1832), 390-393 (Werke **1**, 189-194). [327]

Lejeune Dirichlet, G. (4): Einige neue Sätze über unbestimmte Gleichungen. Abh. K. Preuss. Akad. Wiss. **1834**, 649-664 (Werke **1**, 219-236). [119]

Lejeune Dirichlet, G. (5): Beweis eines Satzes über die arithmetische Progression. Ber. K. Preuss. Akad. Wiss. **1837**, 108-110 (Werke **1**, 307-312). [213]

Lejeune Dirichlet, G. (6) Beweis des Satzes, daß jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Faktor sind, unendlich viele Primzahlen enthält. Abh. K. Preuss. Akad. Wiss. **1837**, 45-81 (Werke **1**, 313-342). [213]

Lejeune Dirichlet, G. (7): Sur la manière de résoudre l'équation $t^2 - pu^2 = 1$ au moyen des fonctions circulaires. J. Reine Angew. Math. **17** (1837), 286-290 (Werke **1**, 343-350). [57, 217]

Lejeune Dirichlet, G. (8): Sur l'usage des séries infinies dans la théorie des nombres. J. Reine Angew. Math. **18** (1838), 259-274 (Werke **1**, 357-374). [57, 140, 142, 150]

Lejeune Dirichlet, G. (9): Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres. J. Reine Angew. Math. **19** (1839), 324-369; **21** (1840), 1-12, 134-155 (Werke **1**, 411-496). [140, 142, 150]

Lejeune Dirichlet, G. (10): Untersuchungen über die Theorie der komplexen Zahlen. Ber. K. Preuss. Akad. Wiss. **1841**, 190-194 (Werke **1**, 503-508). [152, 153]

Lejeune Dirichlet, G. (11): Untersuchungen über die Theorie der komplexen Zahlen. Abh. K. Preuss. Akad. Wiss. **1841**, 141-161 (Werke **1**, 509-532). [152, 153]

Lejeune Dirichlet, G. (12): Recherches sur les formes quadratiques à coefficients et à indéterminées complexes. J. Reine Angew. Math. **24** (1842), 291-371 (Werke **1**, 533-618). [152, 153]

Lejeune Dirichlet, G. (13): Sur la théorie des nombres. C. R. Acad. Sci. Paris **10** (1840), 285-288 (Werke **1**, 619-623). [45]

Lejeune Dirichlet, G. (14): Einige Resultate von Untersuchungen über eine Klasse homogener Funktionen des dritten und der höheren Grade. Ber. K. Preuss. Akad. Wiss. **1841** , 280-285 (Werke **1**, 625-632). [45]

Lejeune Dirichlet, G. (15): Sur un théorème relatif aux séries. J. Math. Pures Appl. Sér. II. **1** (1856), 80-81 (Werke **2**, 195-200). [60]

Lejeune Dirichlet, G. (16): Verallgemeinerung eines Satzes aus der Lehre von den Kettenbrüchen nebst einigen Anwendungen auf die Theorie der Zahlen. Ber. K. Preuss. Akad. Wiss. **1842**, 93–95 (Werke **1**, (1842), 633–638) and Zur Theorie der komplexen Einheiten. Ber. K. Preuss. Akad. Wiss. **1846**, 103–107 (Werke **1**, 639–644). [45]

Eisenstein, G. (1): Über eine neue Gattung zahlentheoretischer Funktionen. Ber. K. Akad. Wiss. Berlin **1850**, 36–42 (Mathematische Werke II, 705–711). [304]

Eisenstein, G. (2): Beweis der allgemeinsten Reziprozitätsgesetze zwischen reellen und komplexen Zahlen. Ber. K. Akad. Wiss. Berlin **1850**, 189–198 (Mathematische Werke II, 712–721). [202]

Eisenstein, G. (3): Über die Anzahl der quadratischen Formen, welche in der Theorie der komplexen Zahlen zu einer reellen Determinante gehören. J. Reine Angew. Math. **27** (1844), 80 (Mathematische Werke I, 6). [152]

Eisenstein, G. (4): Beiträge zur Kreisteilung. J. Reine Angew. Math. **27** (1844), 269–278 (Mathematische Werke I, 45–54). [219]

Eisenstein, G. (5): Beweis des Reziprozitätsgesetzes für die kubischen Reste in der Theorie der aus dritten Wurzeln der Einheit zusammengesetzten komplexen Zahlen. J. Reine Angew. Math. **27** (1844), 289–310 (Mathematische Werke I, 59–80). [304]

Eisenstein, G. (6): Über die Anzahl der quadratischen Formen in den verschiedenen komplexen Theorien. J. Reine Angew. Math. **27** (1844), 311–316 (Mathematische Werke I, 89–94). [152]

Eisenstein, G. (7): Nachtrag zum kubischen Reziprozitätssatze für die aus dritten Wurzeln der Einheit zusammengesetzten komplexen Zahlen. Kriterien des kubischen Charakters der Zahl 3 und ihrer Teiler. J. Reine Angew. Math. **28** (1844), 28–35 (Mathematische Werke I, 81–88). [304]

Eisenstein, G. (8): Lois de reciprocité. Nouvelle démonstration du théorème fondamental sur les résidus quadratiques dans la théorie des nombres complexes. Demonstration du théorème fondamental sur les résidus biquadratiques. Le théorème le plus général sur les caractères biquadratiques, qui comprend comme cas particulier le théorème fondamental. J. Reine Angew. Math. **28** (1844), 53–67 (Mathematische Werke I, 126–140). [304]

Eisenstein, G. (9): Einfacher Beweis und Verallgemeinerung des Fundamentaltheorems für die biquadratischen Reste. J. Reine Angew. Math. **28** (1844), 223–245 (Mathematische Werke I, 141–163). [304]

Eisenstein, G. (10): Allgemeine Untersuchungen über die Formen dritten Grades mit drei Variabeln, welche der Kreisteilung ihre Entstehung verdanken. J. Reine Angew. Math. **28** (1844), 289–374 and **29** (1845), 19–53 (Mathematische Werke I, 167–286). [197, 222]

Eisenstein, G. (11): Zur Theorie der quadratischen Zerfällung der Primzahlen $8n+3$, $7n+2$ und $7n+4$. J. Reine Angew. Math. **37** (1848), 97–126 (Mathematische Werke II, 506–535). [220]

Eisenstein, G. (12): Über ein einfaches Mittel zur Auffindung der höheren Reziprozitätsgesetze und der mit ihnen zu verbindenden Ergänzungssätze. J. Reine Angew. Math. **39** (1850), 351–364 (Mathematische Werke II, 623–636). [304]

Frobenius, G. (1): Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe. Ber. K. Akad. Wiss. Berlin **1896**, 689–703 (Gesammelte Abhandlungen **2**, 719–733). [95]

Fuchs, L. (1): Über die Perioden, welche aus den Wurzeln der Gleichung $\omega^n = 1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist. J. Reine Angew. Math. **61** (1863), 374–386 (Werke I, 53–66). [197]

Fuchs, L. (2): Über die aus Einheitswurzeln gebildeten komplexen Zahlen von periodischem Verhalten, insbesondere die Bestimmung der Klassenanzahl derselben. J. Reine Angew. Math. **65** (1866), 74–111 (Werke I, 69–109). [197]

Gauss, C. F. (1): Disquisitiones arithmeticæ. Leipzig 1801. English translation, New Haven 1966. (Werke **1**, 10–474). [119, 127, 128, 134, 135, 140]

Gauss, C. F. (2): Summatio quarundam serierum singularium (Werke **2**, 11–45). [221]

Gauss, C. F. (3): Theoria residuorum biquadraticorum, commentatio prima et secunda (Werke **2**, 65–92 and 93–148). [304]

Gmeiner, J. A. (1): Die Ergänzungssätze zum bikubischen Reziprozitätsgesetze. Ber. K. Akad. Wiss. Wien **100** (1891), 1330–1361. [304]

Gmeiner, J. A. (2): Das allgemeine bikubische Reziprozitätsgesetz. Ber. K. Akad. Wiss. Wien **101** (1892), 562–584. [304]

Gmeiner, J. A. (3): Die bikubische Reziprozität zwischen einer reellen und einer zweigliedrigen regulären Zahl. Monatsh. Math. Phys. **3** (1892), 199–210. [304]

Hensel, K. (1): Arithmetische Untersuchungen über Diskriminanten und ihre außerwesentlichen Teiler. Inaugural-Dissert. Berlin **1884**. [32]

Hensel, K. (2): Darstellung der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor. J. Reine Angew. Math. **101** (1887), 99–141 and **103** (1888), 230–237. [32]

Hensel, K. (3): Über Gattungen, welche durch Komposition aus zwei anderen Gattungen enstehen. J. Reine Angew. Math. **105** (1889), 329–344. [99]

Hensel, K. (4): Untersuchung der Fundamentalgleichung einer Gattung für eine reelle Primzahl als Modul und Bestimmung der Teiler ihrer Diskriminante. J. Reine Angew. Math. **113** (1894), 61–83. [25, 30]

Hensel, K. (5): Arithmetische Untersuchungen über die gemeinsamen außerwesentlichen Diskriminantenteiler einer Gattung. J. Reine Angew. Math. **113** (1894), 128–160. [32]

Hermite, C. (1): Sur la théorie des formes quadratiques ternaires indéfinies. J. Reine Angew. Math. **47** (1854), 307–312 (Œuvres **1**, 193–199). [43]

Hermite, C. (2): Extrait d'une lettre de M. Ch. Hermite à M. Borchardt sur le nombre limité d'irrationalités auxquelles se réduisent les racines des équations à coefficients entiers complexes d'un degré et d'un discriminant donnés. J. Reine Angew. Math. **53** (1857), 182–192 (Œuvres **1**, 415–428). [43]

Hilbert, D. (2): Zwei neue Beweise für die Zerlegbarkeit der Zahlen eines Körpers in Primideale. Jahresber. Deutsch. Math.-Verein. **3** (1894), 59 (Gesammelte Abhandlungen **1**, 5). [15, 79]·

Hilbert, D. (3): Über die Zerlegung der Ideale eines Zahlkörpers in Primideale. Math. Ann. **44** (1894), 1–8 (Gesammelte Abhandlungen **1**, 6–12). [15, 79, 80]

Hilbert, D. (4): Grundzüge einer Theorie des Galoischen Zahlkörpers. Nachr. K. Ges. Wiss. Göttingen **1894**, 224–236 (Gesammelte Abhandlungen **1**, 13–23). [35, 81]

Hilbert, D. (5): Über den Dirichletschen biquadratischen Zahlkörper. Math. Ann. **45** (1894), 309–340 (Gesammelte Abhandlungen **1**, 24–52). [152, 153]

Hilbert, D. (6): Ein neuer Beweis des Kroneckerschen Fundamentalsatzes über Abelsche Zahlkörper. Nachr. K. Ges. Wiss. Göttingen **1896**, 29–39 (Gesammelte Abhandlungen **1**, 53–62). [176]

Hurwitz, A. (1): Über die Theorie der Ideale. Nachr. K. Ges. Wiss. Göttingen **1894**, 291–298 (Mathematische Werke **2**, 191–197). [12]

Hurwitz, A. (2): Über einen Fundamentalsatz der arithmetischen Theorie der algebraischen Grössen. Nachr. K. Ges. Wiss. Göttingen **1895**, 230–240 (Mathematische Werke **2**, 198–207). [12]

Hurwitz, A. (3): Zur Theorie der algebraischen Zahlen. Nachr. K. Ges. Wiss. Göttingen **1895**, 324–331 (Mathematische Werke **2**, 236–243). [16]

Hurwitz, A. (4): Die unimodularen Substitutionen in einem algebraischen Zahlkörper. Nachr. K. Ges. Wiss. Göttingen **1895**, 332–356 (Mathematische Werke **2**, 244–268). [55]

Jacobi, C. G. J. (1): De residuis cubicis commentatio numerosa. J. Reine Angew. Math. **2** (1827), 66–69 (Gesammelte Werke **6**, 233–237). [219, 304]

Jacobi, C. G. J. (2): Observatio arithmetica de numero classium divisorum quadraticorum formae $y^2 + Az^2$ designante A numerum primum formae $4n + 3$. J. Reine Angew. Math. **9** (1832), 189–192 (Gesammelte Werke **6**, 240–244). [219]

Jacobi, C. G. J. (3): Über die Kreisteilung und ihre Anwendung auf die Zahlentheorie. J. Reine Angew. Math. **30** (1846), 166–182 (Gesammelte Werke **6**, 254–274). [196, 219]

Jacobi, C. G. J. (4): Über die komplexen Primzahlen, welche in der Theorie der Reste der 5ten, 8ten und 12ten Potenzen zu betrachten sind. J. Reine Angew. Math. **19** (1839), 314–318 (Gesammelte Werke **6**, 275–280). [219, 304]

Kronecker, L. (1): De unitatibus complexis. Dissertatio inauguralis. Berolini 1845. J. Reine Angew. Math. **93** (1882), 1–52 (Werke **1**, 5–73). [105]

Kronecker, L. (2): Über die algebraisch auflösbaren Gleichungen (I. Abhandlung). Ber. K. Akad. Wiss. Berlin **1853**, 365–374 (Werke **4**, 1–11). [176]

Kronecker, L. (3): Mémoire sur les facteurs irréductibles de l'expression $x^n - 1$. J. Math. Pures Appl. Sér. I. **19** (1854), 177–192 (Werke **1**, 75–92). [171]

Kronecker, L. (4): Sur une formule de Gauss. J. Math. Pures Appl. Sér. II. **1** (1856), 392–395 (Werke **4**, 171–175). [221]

Kronecker, L. (5): Démonstration d'un théorème de M. Kummer. J. Math. Pures Appl. Sér. II. **1** (1856), 396–398 (Werke **1**, 93–97). [257]

Kronecker, L. (6): Zwei Sätze über Gleichungen mit ganzzahligen Koeffizienten. J. Reine Angew. Math. **53** (1857), 173–175 (Werke **1**, 103–108). [51]

Kronecker, L. (7): Über komplexe Einheiten. J. Reine Angew. Math. **53** (1857), 176–181 (Werke **1**, 109–118). [173]

Kronecker, L. (8): Über kubische Gleichungen mit rationalen Koeffizienten. J. Reine Angew. Math. **56** (1859), 188 (Werke **1**, 119–122). [333]

Kronecker, L. (9): Über die Klassenanzahl der aus Wurzeln der Einheit gebildeten komplexen Zahlen. Ber. K. Akad. Wiss. Berlin **1863**, 340–345 (Werke **1**, 123–131). [210]

Kronecker, L. (10): Über den Gebrauch der Dirichlet'schen Methoden in der Theorie der quadratischen Formen. Ber. K. Akad. Wiss. Berlin **1864**, 285–303 (Werke **4**, 227–244). [142]

Kronecker, L. (11): Auseinandersetzung einiger Eigenschaften der Klassenanzahl idealer komplexer Zahlen. Ber. K. Akad. Wiss. Berlin **1870**, 881–889 (Werke **1**, 271–282). [62, 210]

Kronecker, L. (12): Bemerkungen zu Reuschle's Tafeln komplexer Primzahlen. Ber. K. Akad. Wiss. Berlin **1875**, 236–238 (Werke **5**, 449–452). [215]

Kronecker, L. (13): Über Abelsche Gleichungen. Ber. K. Akad. Wiss. Berlin **1877**, 845–851 (Werke **4**, 63–71). [176]

Kronecker, L. (14): Über die Irreduktibilität von Gleichungen. Ber. K. Akad. Wiss. Berlin **1880**, 155–162 (Werke **2**, 83–93). [94, 96]

Kronecker, L. (15): Über die Potenzreste gewisser komplexer Zahlen. Ber. K. Akad. Wiss. Berlin **1880**, 404–407 (Werke **2**, 95–101). [217]

Kronecker, L. (16): Grundzüge einer arithmetischen Theorie der algebraischen Grössen. J. Reine Angew. Math. **92** (1882), 1–122 (Werke **2**, 237–387). [3, 5, 7, 14, 25, 30, 32, 54]

Kronecker, L. (17): Zur Theorie der Abelschen Gleichungen. Bemerkungen zum vorangehenden Aufsatz des Herrn Schwering. J. Reine Angew. Math. **93** (1882), 338–364 (Werke **4**, 131–162). [197]

Kronecker, L. (18): Sur les unités complexes (3 notes). C. R. Acad. Sci. Paris **96** (1883), 93–98, 148–152, 216–221 (Werke **3**, 1–19). (See also J. Molk: Sur les unités complexes. Bull. sciences math. astron. **1883**). [45]

Kronecker, L. (19): Zur Theorie der Formen höherer Stufen. Ber. K. Akad. Wiss. Berlin **1883**, 957–960 (Werke **2**, 417–424). [12]

Kronecker, L. (20): Additions au mémoire sur les unités complexes. C. R. Acad. Sci. Paris **99** (1884), 765–771 (Werke **3**, 21–30). [45]

Kronecker, L. (21): Ein Satz über Diskriminanten-Formen. J. Reine Angew. Math. **100** (1886), 79–82 (Werke **3**, 241–247). [171]

Kummer, E. (1): De aequatione $x^{2\lambda} + y^{2\lambda} = z^{2\lambda}$ per numeros integros resolvenda. J. Reine Angew. Math. **17** (1837), 203–209 (Collected Papers **1**, 135–141). [327]

Kummer, E. (2): Eine Aufgabe, betreffend die Theorie der kubischen Reste. J. Reine Angew. Math. **23** (1842), 285–286 (Collected Papers **1**, 143–144). [197]

Kummer, E. (3): Über die Divisoren gewisser Formen der Zahlen, welche aus der Theorie der Kreisteilung entstehen. J. Reine Angew. Math. **30** (1846), 107–111 (Collected Papers **1**, 193–202). [197]

Kummer, E. (4): De residuis cubicis disquisitiones nonnullae analyticae. J. Reine Angew. Math. **32** (1846), 341–359 (Collected Papers **1**, 145–163). [197]

Kummer, E. (5): Zur Theorie der komplexen Zahlen. J. Reine Angew. Math. **35** (1847), 319–326 (Collected Papers **1**, 203–210). [9, 164]

Kummer, E. (6): Über die Zerlegung der aus Wurzeln der Einheit gebildeten komplexen Zahlen in ihre Primfaktoren. J. Reine Angew. Math. **35** (1847), 327–367 (Collected Papers **1**, 211–251). [9, 103, 164, 192, 193, 197]

Kummer, E. (7): Bestimmung der Anzahl nicht äquivalenter Klassen für die aus λ-ten Wurzeln der Einheit gebildeten komplexen Zahlen und die idealen Faktoren derselben. J. Reine Angew. Math. **40** (1850), 93–116 (Collected Papers **1**, 299–322). [210]

Kummer, E. (8): Zwei besondere Untersuchungen über die Klassenanzahl und über die Einheiten der aus λ-ten Wurzeln der Einheit gebildeten komplexen Zahlen. J. Reine Angew. Math. **40** (1850), 117–129 (Collected Papers **1**, 323–335). [257, 262, 265]

Kummer, E. (9): Allgemeiner Beweis des Fermat'schen Satzes, daß die Gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen unlösbar ist, für alle diejenigen Potenz-Exponenten λ, welche ungerade Primzahlen sind und in der Zählern der ersten $\frac{1}{2}(\lambda - 3)$ Bernoulli'schen Zahlen als Faktoren nicht vorkommen. J. Reine Angew. Math. **40** (1850), 130–138 (Collected Papers **1**, 336–344). [327]

Kummer, E. (10): Allgemeine Reziprozitätsgesetze für beliebig hohe Potenzreste. Ber. K. Akad. Wiss. Berlin **1850**, 154–165 (Collected Papers **1**, 345–357). [199, 290]

Kummer, E. (11): Mémoire sur la théorie des nombres complexes composés de racines de l'unité et des nombres entiers. J. Math. Pures Appl. Sér. I. **16** (1851), 377–498 (Collected Papers **1**, 363–484). [192, 193, 197, 210, 264, 327]

Kummer, E. (12): Über die Ergänzungssätze zu den allgemeinen Reziprozitätsgesetzen. J. Reine Angew. Math. **44** (1852), 93–146 (Collected Papers **1**, 485–538). [241, 260, 266, 290]

Kummer, E. (13): Über die Irregularität der Determinanten. Ber. K. Akad. Wiss. Berlin **1853**, 194–200 (Collected Papers **1**, 539–545). [197, 211]

Kummer, E. (14): Über eine besondere Art, aus komplexen Einheiten gebildeter Ausdrücke. J. Reine Angew. Math. **50** (1855), 212–232 (Collected Papers **1**, 552–572). [109]

Kummer, E. (15): Theorie der idealen Primfaktoren der komplexen Zahlen, welche aus den Wurzeln der Gleichung $\omega^n = 1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist. Abh. K. Akad. Wiss. Berlin **1856**, 1–47 (Collected Papers **1**, 583–629). [170]

Kummer, E. (16): Einige Sätze über die aus den Wurzeln der Gleichung $\alpha^\lambda = 1$ gebildeten komplexen Zahlen, für den Fall, daß die Klassenanzahl durch λ teilbar ist, nebst Anwendung derselben auf einem weiteren Beweis des letzten Fermat'schen Lehrsatzes. Abh. K. Akad. Wiss. Berlin **1857**, 41–74 (Collected Papers **1**, 639–672). [332]

Kummer, E. (17): Über die den Gaussischen Perioden der Kreisteilung entsprechenden Kongruenzwurzeln. J. Reine Angew. Math. **53** (1857), 142–148 (Collected Papers **1**, 573–580). [197]

Kummer, E. (18): Über die allgemeinen Reziprozitätsgesetze der Potenzreste. Ber. K. Akad. Wiss. Berlin **1858**, 158–171 (Collected Papers **1**, 673–687). [290]

Kummer, E. (19): Über die Ergänzungssätze zu den allgemeinen Reziprozitätsgesetzen. J. Reine Angew. Math. **56** (1859), 270–279 (Collected Papers **1**, 688–697). [290]

Kummer, E. (20): Über die allgemeinen Reziprozitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist. Abh. K. Akad. Wiss. Berlin **1859**, 19–159 (Collected Papers **1**, 699–839). [109, 242, 245, 246, 254, 290, 308]

Kummer, E. (21): Zwei neue Beweise der allgemeinen Reziprozitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist. J. Reine Angew. Math. **100** (1887), 10–50 (Collected Papers **1**, 842–882). [109, 290]

Kummer, E. (22): Über die Klassenanzahl der aus n-ten Einheitswurzeln gebildeten komplexen Zahlen. Ber. K. Akad. Wiss. Berlin **1861**, 1051–1053 (Collected Papers **1**, 883–885). [210]

Kummer, E. (23): Über die Klassenanzahl der aus zusammengesetzten Einheitswurzeln gebildeten idealen komplexen Zahlen. Ber. K. Akad. Wiss. Berlin **1863**, 21–28 (Collected Papers **1**, 887–894). [210]

Kummer, E. (24): Über die einfachste Darstellung der aus Einheitswurzeln gebildeten komplexen Zahlen, welche durch Multiplikation mit Einheiten bewirkt werden kann. Ber. K. Akad. Wiss. Berlin **1870**, 409–420 (Collected Papers **1**, 895–906). [215]

Kummer, E. (25): Über eine Eigenschaft der Einheiten der aus den Wurzeln der Gleichung $\alpha^\lambda = 1$ gebildeten komplexen Zahlen, und über den zweiten Faktor der Klassenzahl. Ber. K. Akad. Wiss. Berlin **1870**, 855–880 (Collected Papers **1**, 919–944). [210]

Kummer, E. (26): Über diejenigen Primzahlen λ, für welche die Klassenzahl der aus λ-ten Einheitswurzeln gebildeten komplexen Zahlen durch λ teilbar ist. Ber. K. Akad. Wiss. Berlin **1874**, 239–248 (Collected Papers **1**, 945–954). [264]

Lagrange, J. L. (1): Sur la solution des problèmes indéterminés du second degré. Mem. Acad. R. Sci. Berlin **23** (1796) (Œuvres **2** (1868) 375–535). [133, 134]

Lamé, G. (1): Mémoire d'analyse indéterminée démontrant que l'équation $x^7 + y^7 = z^7$ est impossible en nombres entiers. J. Math. Pures Appl. **5** (1840), 195–211. [327]

Lamé, G. (2): Mémoire sur la résolution, en nombres complexes, de l'équation $A^5 + B^5 + C^5 = 0$. J. Math. Pures Appl. **12** (1847), 137–171. [327]

Lamé, G. (3): Mémoire sur la résolution, en nombres complexes, de l'équation $A^n + B^n + C^n = 0$. J. Math. Pures Appl. **12** (1847), 172–184. [327]

Lebesgue, V. A. (1): Démonstration de l'impossibilité de résoudre l'équation $x^7 + y^7 + z^7 = 0$ en nombers entiers. J. Math. Pures Appl. **5** (1840), 276–279. [327]

Lebesgue, V. A. (2): Addition à la note sur l'équation $x^7 + y^7 + z^7 = 0$. J. Math. Pures Appl. **5** (1840), 348–349. [327]

Lebesgue, V. A. (3): Théorèmes nouveaux sur l'équation indéterminée $x^5 + y^5 = az^5$. J. Math. Pures Appl. **8** (1843), 49–70. [327]

Legendre, A. (1): Essai sur la théorie des nombres. Paris, 1798. [119, 134]

Mertens, F. (1): Über einen algebraischen Satz. Ber. K. Akad. Wiss. Wien **1892**. [12]

Minkowski, H. (1): Über die positiven quadratischen Formen und über kettenbruchähnliche Algorithmen. J. Reine Angew. Math. **107** (1891), 278–297 (Gesammelte Abhandlungen **1**, 243–260). [43, 44, 54]

Minkowski, H. (2): Théorèmes arithmétiques. Extrait d'une lettre à M. Hermite. C. R. Acad. Sci. Paris **112** (1891), 209–212 (Gesammelte Abhandlungen **1**, 261–263). [43, 44]

Minkowski, H. (3): Geometrie der Zahlen. Leipzig, 1896. [41, 43, 44, 45, 51, 52, 54]

Minkowski, H. (4): Généralisation de la théorie des fractions continues. Ann. l'école normale supérieure Sér. 3, **13** (1896), 41–60 (Zur Theorie der Kettenbrüche, Gesammelte Abhandlungen **1**, 278–292). [52]

Minnigerode, C. (1): Über die Verteilung der quadratischen Formen mit komplexen Koeffizienten und Veränderlichen in Geschlechter. Nachr. K. Ges. Wiss. Göttingen **1873**. [152, 153]

Reuschle, C. G. (1): Tafeln komplexer Primzahlen, welche aus Wurzeln der Einheit gebildet sind. Berlin, 1875. [215]

Schering, E. (1): Zahlentheoretische Bemerkung. Auszug aus einem Brief an Herrn Kronecker. J. Reine Angew. Math. **100** (1887),447–448 (Gesammelte Mathematische Werke I, 103–104). [62]

Schering, E. (2): Die Fundamentalklassen der zusammensetzbaren arithmetischen Formen. Abh. K. Akad. Wiss. Göttingen **14** (1869), 3–16 (Gesammelte Mathematische Werke I, 135–148).

Schwering, K. (1): Zur Theorie der arithmetischen Funktionen, welche von Jacobi $\psi(\alpha)$ genannt werden. J. Reine Angew. Math. **93** (1882), 334–337. [197]

Schwering, K. (2): Untersuchung über die fünften Potenzreste und die aus fünften Einheitswurzeln gebildeten ganzen Zahlen. Z. Math. Phys. **27** (1882), 102–119. [197]

Schwering, K. (3): Über gewisse trinomische komplexe Zahlen. Acta Math. **10** (1887), 57–86. [197]

Schwering, K. (4): Eine Eigenschaft der Primzahl 107. Acta Math. **11** (1887), 119–120. [197]

Serret, J.-A. (1): Cours d'algèbre supérieure Tome 2, Section 3. Paris, 1849. [26]

Smith, H. J. S. (1): Report on the theory of numbers (1859–1865) (Collected Mathematical Papers **1**, 38–364). [197]

Stickelberger, L. (1): Über eine Verallgemeinerung der Kreisteilung. Math. Ann. **37** (1890), 321–367. [220]

Tano, F. (1): Sur quelques théorèmes de Dirichlet. J. Reine Angew. Math. **105** (1889), 160–169. [119]

Weber, H. (1): Theorie der Abelschen Zahlkörper. Acta Math. **8** (1886), 193–263; ibid. **9** (1887), 105–130. [176, 197, 210]

Weber, H. (2): Über Abelsche Zahlkörper dritten und vierten Grades. Sitzungsber. Ges. Naturwiss. Marburg **1892**. [197, 222]

Weber, H. (3): Zahlentheoretische Untersuchungen aus dem Gebiete der elliptischen Funktionen. Nachr. K. Ges. Wiss. Göttingen **1893**.

Weber, H. (4): Lehrbuch der Algebra **2**. Braunschweig 1896. [150, 170, 197, 210, 222]

Wolfskehl, P. (1): Beweis, daß der zweite Faktor der Klassenanzahl für die aus den elften und dreizehnten Einheitswurzeln gebildeten Zahlen gleich eins ist. J. Reine Angew. Math. **99** (1886), 173–178. [197]

List of Theorems and Lemmas

Index